EUROPEISKA
KOMMISSIONEN

Bryssel den 13.3.2024
C(2024) 1532 final

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 13.3.2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar verktyg, metoder, processer och strategier för IKT-riskhantering och den förenklade IKT-riskhanteringsramen

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL DEN DELEGERADE AKTEN

Ett av målen med förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn är att fastställa enhetliga krav för säkerheten i nätverks- och informationssystem hos företag och organisationer som är verksamma inom finanssektorn. Därigenom skapas ett regelverk om digital operativ motståndskraft, där alla finansiella entiteter måste säkerställa att de kan stå emot, reagera på och återställa sig från alla typer av IKT-relaterade avbrott och hot. Dessa krav är enhetliga i hela EU och syftar till att förebygga och minska cyberhot.

I detta avseende ska de europeiska tillsynsmyndigheterna enligt artikel 15 första stycket i förordningen om digital operativ motståndskraft för finanssektorn ”genom den gemensamma kommittén och i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta gemensamma förslag till tekniska standarder för tillsyn” i syfte att ytterligare säkerställa ”harmonisering av verktyg, metoder, processer och strategier för IKT-riskhantering” och, enligt artikel 16, utarbeta en förenklad IKT-riskhanteringsram för vissa finansiella entiteter. Enisa har följaktligen varit involverad i underkommittén för digital operativ motståndskraft inom den gemensamma kommittén för de europeiska tillsynsmyndigheterna.

Denna delegerade förordning motsvarar detta mandat och överlämnades till kommissionen den 17 januari 2024.

2. SAMRÅD SOM FÖREGÅTT ANTAGANDET AV AKTEN

Som ett led i utarbetandet av de standarder som anges i detta förslag till förordning offentliggjorde de europeiska tillsynsmyndigheterna den 19 juni 2023 ett förslag till tekniska standarder för tillsyn för en samrådsperiod på tre månader, som avslutades den 11 september 2023. De europeiska tillsynsmyndigheterna mottog 120 svar från en mängd olika marknadsaktörer inom hela finanssektorn. De europeiska tillsynsmyndigheternas slutrapport innehåller en fullständig översikt över svaren från berörda parter[1].

De som svarade på det offentliga samrådet efterlyste i sina kommentarer följande när det gäller förslagen till tekniska standarder för tillsyn:

- Att förlänga tidsfristen för genomförandet.
- Att uppnå starkare proportionalitet (t.ex. proportionalitet åt båda hållen, dvs. att man tar hänsyn till både ökad och minskad komplexitet och ökade och minskade risker och ett mer sektorsspecifikt tillvägagångssätt med ytterligare proportionalitet för t.ex. försäkringsföretag m.m.).
- Att styrningsaspekter undantas från förslaget till tekniska standarder för tillsyn eftersom de verkar ligga utanför mandatet.
- Att inte överväga ytterligare åtgärder för molnbaserade datorresurser.

Mot bakgrund av de mottagna kommentarerna införde de europeiska tillsynsmyndigheterna ändringar i förslaget till tekniska standarder för tillsyn. Dessa ändringar gällde t.ex. införandet av ytterligare proportionalitet, strykningen av artikeln om styrning från de allmänna systemkraven och förtydligande av bestämmelser, särskilt de som ingår i artiklarna om

[1] De europeiska tillsynsmyndigheterna (2024), *Final report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554* (inte översatt till svenska).

nätverkssäkerhet, kryptering, åtkomstkontroll och driftskontinuitet. De europeiska tillsynsmyndigheterna beslutade att inte ta med specifika inslag om molntjänster för att följa principen om att säkerställa teknikneutralitet. I stället beslutade de europeiska tillsynsmyndigheterna att bredda de övervägda kraven till att omfatta IKT-tillgångar eller tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster i allmänhet. När det gäller tidsfristerna för genomförande övervägde de europeiska tillsynsmyndigheterna dock inte några ändringar eftersom dessa fastställs på nivå 1 i förordningen om digital operativ motståndskraft för finanssektorn.

3. DEN DELEGERADE AKTENS RÄTTSLIGA ASPEKTER

I avdelning I kapitel I fastställs huvudprincipen och de faktorer som ska beaktas vid utarbetande och genomförande av IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg (artikel 1).

I avdelning II kapitel I fastställs villkoren för ytterligare harmonisering av verktyg, metoder, processer och strategier för IKT-riskhantering, genom att det fastställer allmänna delar av IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg (avsnitt 1); särskilda delar av IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg (avsnitt 2); risktoleransnivå, metoder för att genomföra IKT-riskbedömningen, IKT-riskhanteringsåtgärder, en policy för hantering av IKT-tillgångar (avsnitt 3); en policy för kryptering och kryptografisk säkerhet (avsnitt 4); en säkerhetsstrategi för IKT-verksamhet (avsnitt 5); en policy för hantering av nätverkssäkerhet (avsnitt 6); en policy för IKT-projekthantering (avsnitt 7); och en policy för fysisk säkerhet och miljösäkerhet för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet (avsnitt 8). I kapitel II fastställs alla delar av IKT-säkerheten som de finansiella entiteterna ska inkludera i utarbetandet av sin strategi för personalresurser och sin strategi för åtkomstkontroll. I kapitel III fastställs alla delar av en policy för upptäckt och hantering av IKT-relaterade incidenter som de finansiella entiteterna ska utarbeta och genomföra. I kapitel IV fastställs innehållet i och formatet för den rapport om översynen av IKT-riskhanteringsramen som de finansiella entiteterna ska utarbeta och överlämna.

I avdelning III fastställs en förenklad IKT-riskhanteringsram med fokus på inrättande av en styrnings- och kontrollram (kapitel I), mekanismer och krav för åtkomst och kontroll (kapitel II), inrättande av en IKT-kontinuitetsplan (kapitel III), och fastställande av innehållet i och formatet för den rapport om översynen av IKT-riskhanteringsramen som de finansiella entiteterna ska utarbeta och överlämna (kapitel IV).

Avdelning IV innehåller slutbestämmelser om aktens ikraftträdande (artikel 42).

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 13.3.2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar verktyg, metoder, processer och strategier för IKT-riskhantering och den förenklade IKT-riskhanteringsramen

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011[2], särskilt artiklarna 15 fjärde stycket och 16.3 fjärde stycket, och

av följande skäl:

(1) Förordning (EU) 2022/2554 omfattar ett brett spektrum av finansiella entiteter som skiljer sig åt i fråga om storlek, struktur, intern organisation och verksamhetens karaktär och komplexitet, och som därmed har delar av ökad eller minskad komplexitet eller ökade eller minskade risker. För att säkerställa att denna variation vederbörligen beaktas bör alla krav avseende IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg och avseende en förenklad IKT-riskhanteringsram stå i proportion till dessa finansiella entiteters storlek, struktur, interna organisation, karaktär och komplexitet samt till de motsvarande riskerna.

(2) Av samma skäl bör finansiella entiteter som omfattas av förordning (EU) 2022/2554 ha en viss flexibilitet när det gäller hur de uppfyller kraven avseende IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg, och avseende en förenklad IKT-riskhanteringsram. Finansiella entiteter bör därför tillåtas att använda all dokumentation som de redan har för att uppfylla samtliga dokumentationskrav som följer av dessa krav. Av detta följer att utarbetande, dokumentation och genomförande av specifika IKT-relaterade säkerhetsstrategier endast bör krävas för vissa väsentliga delar, med beaktande av bland annat ledande branschpraxis och branschstandarder. För att tillgodose specifika tekniska genomförandeaspekter är det dessutom nödvändigt att utarbeta, dokumentera och genomföra IKT-säkerhetsförfaranden, inbegripet kapacitets- och prestandahantering, hantering av sårbarheter och programfixar, data- och systemsäkerhet samt loggning.

(3) För att säkerställa ett korrekt genomförande över tid av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i avdelning II kapitel

[2] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

I i denna förordning är det viktigt att finansiella entiteter på ett korrekt sätt fördelar och upprätthåller alla roller och ansvarsområden som rör IKT-säkerhet, och att de fastställer konsekvenserna av bristande efterlevnad av IKT-relaterade säkerhetsstrategier eller säkerhetsförfaranden.

(4) För att begränsa risken för intressekonflikter bör de finansiella entiteterna säkerställa åtskillnad av arbetsuppgifter när de fördelar roller och ansvarsområden på IKT-området.

(5) För att säkerställa flexibilitet och förenkla de finansiella entiteternas kontrollram bör finansiella entiteter inte vara skyldiga att utarbeta särskilda bestämmelser om konsekvenserna av bristande efterlevnad av de IKT-relaterade säkerhetsstrategier, förfaranden och protokoll som avses i avdelning II kapitel I i denna förordning om sådana bestämmelser redan fastställs i en annan strategi eller ett annat förfarande.

(6) I en dynamisk miljö där IKT-riskerna ständigt utvecklas är det viktigt att finansiella entiteter utvecklar sin uppsättning IKT-relaterade säkerhetsstrategier på grundval av ledande praxis och, i tillämpliga fall, standarder enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012[3]. Detta bör göra det möjligt för de finansiella entiteter som avses i avdelning II i denna förordning att förbli informerade och förberedda i en föränderlig miljö.

(7) För att säkerställa sin digitala operativa motståndskraft bör de finansiella entiteter som avses i avdelning II i denna förordning, som en del av sina IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg, utarbeta och genomföra en policy för hantering av IKT-tillgångar, förfaranden för kapacitets- och prestandahantering samt strategier och förfaranden för IKT-verksamhet. Dessa strategier och förfaranden är nödvändiga för att säkerställa övervakningen av IKT-tillgångarnas status under hela deras livscykel, så att dessa tillgångar används och underhålls på ett ändamålsenligt sätt (hantering av IKT-tillgångar). Strategierna och förfarandena bör också säkerställa att driften av IKT-systemen optimeras och att IKT-systemens och IKT-kapacitetens prestanda uppfyller de fastställda verksamhets- och informationssäkerhetsmålen (kapacitets- och prestandahantering). Slutligen bör strategierna och förfarandena säkerställa en effektiv och smidig daglig hantering och drift av IKT-systemen (IKT-verksamhet) och därigenom minimera risken för att uppgifternas konfidentialitet, integritet och tillgänglighet förloras. Dessa strategier och förfaranden är således nödvändiga för att säkerställa nätverkssäkerheten, tillhandahålla lämpliga skyddsåtgärder mot intrång och missbruk av uppgifter samt bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet.

(8) För att säkerställa en korrekt hantering av risken med äldre IKT-system bör finansiella entiteter registrera och övervaka slutdatum för IKT-supporttjänster från tredje part. På grund av den potentiella inverkan som en förlust av uppgifternas konfidentialitet, integritet och tillgänglighet kan ha, bör finansiella entiteter fokusera på de IKT-tillgångar eller IKT-system som är kritiska för affärsverksamheten när de registrerar och övervakar dessa slutdatum.

---

[3] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(9) Kryptografiska säkerhetsåtgärder kan säkerställa uppgifters tillgänglighet, äkthet, integritet och konfidentialitet. Finansiella entiteter som avses i avdelning II i denna förordning bör därför identifiera och genomföra sådana åtgärder baserat på en riskbaserad metod. I detta syfte bör de finansiella entiteterna kryptera de berörda uppgifterna i vila, under överföring eller, vid behov, i bruk, baserat på resultaten av en tvådelad process, nämligen dataklassificering och en heltäckande IKT-riskbedömning. Med tanke på komplexiteten i att kryptera uppgifter i bruk bör de finansiella entiteter som avses i avdelning II i denna förordning endast kryptera uppgifter i bruk om det är lämpligt mot bakgrund av resultaten av IKT-riskbedömningen. De finansiella entiteter som avses i avdelning II i denna förordning bör dock, om kryptering av uppgifter i bruk inte är genomförbar eller är alltför komplex, kunna skydda de berörda uppgifternas konfidentialitet, integritet och tillgänglighet genom andra IKT-säkerhetsåtgärder. Med tanke på den snabba tekniska utvecklingen inom området för krypteringsmetoder bör de finansiella entiteter som avses i avdelning II i denna förordning hålla sig à jour med den relevanta utvecklingen inom kryptoanalys och beakta ledande praxis och standarder. De finansiella entiteter som avses i avdelning II i denna förordning bör därför följa en flexibel strategi, baserad på riskreducering och riskövervakning, för att hantera den dynamiska utvecklingen av kryptografiska hot, inbegripet hot från framsteg inom kvantteknik.

(10) En säkerhetsstrategi för IKT-verksamhet och IKT-relaterade strategier, förfaranden, protokoll och verktyg är nödvändiga för att säkerställa uppgifternas konfidentialitet, integritet och tillgänglighet. En central aspekt är den strikta separeringen av IKT-produktionsmiljöer från de miljöer där IKT-system utvecklas och testas eller andra miljöer som inte är produktionsmiljöer. Denna separering bör fungera som en viktig IKT-säkerhetsåtgärd mot oavsiktlig och obehörig åtkomst till, ändringar av och radering av uppgifter i produktionsmiljön, vilket skulle kunna leda till allvarliga avbrott i affärsverksamheten för de finansiella entiteter som avses i avdelning II i denna förordning. Med tanke på nuvarande praxis för utveckling av IKT-system bör finansiella entiteter dock i undantagsfall tillåtas att testa i produktionsmiljöer, förutsatt att de motiverar sådan testning och erhåller det godkännande som krävs.

(11) Den snabba utvecklingen inom IKT-området och i fråga om IKT-sårbarheter och cyberhot kräver en proaktiv och heltäckande strategi för att identifiera, utvärdera och åtgärda IKT-sårbarheter. Utan en sådan strategi kan finansiella entiteter och deras kunder, användare eller motparter vara allvarligt utsatta för risker, vilket skulle äventyra deras digitala operativa motståndskraft, säkerheten i deras nätverk och tillgängligheten, äktheten, integriteten och konfidentialiteten för uppgifter som IKT-relaterade säkerhetsstrategier och förfaranden bör skydda. Finansiella entiteter som avses i avdelning II i denna förordning bör därför identifiera och åtgärda sårbarheter i sin IKT-miljö, och både de finansiella entiteterna och deras tredjepartsleverantörer av IKT-tjänster bör följa en sammanhängande, transparent och ansvarsfull ram för sårbarhetshantering. Av samma skäl bör finansiella entiteter övervaka IKT-sårbarheter med hjälp av tillförlitliga resurser och automatiserade verktyg, och kontrollera att tredjepartsleverantörer av IKT-tjänster vidtar omedelbara åtgärder mot sårbarheter i tillhandahållna IKT-tjänster.

(12) Hantering av programfixar bör vara en viktig del av de IKT-relaterade säkerhetsstrategier och förfaranden som, genom testning och användning i en kontrollerad miljö, ska åtgärda identifierade sårbarheter och förhindra avbrott på grund av installation av programfixar.

(13) För att säkerställa snabb och transparent kommunikation av potentiella säkerhetshot som kan påverka den finansiella entiteten och dess berörda parter, bör finansiella entiteter fastställa förfaranden för ansvarsfullt offentliggörande av IKT-sårbarheter till kunder, motparter och allmänheten. Vid upprättandet av dessa förfaranden bör finansiella entiteter beakta olika faktorer, däribland hur allvarlig sårbarheten är, den potentiella effekten av en sådan sårbarhet på berörda parter och beredskapen för en justering eller begränsningsåtgärder.

(14) För att möjliggöra tilldelning av åtkomsträttigheter för användare bör de finansiella entiteter som avses i avdelning II i denna förordning införa kraftfulla åtgärder för att säkerställa unik identifiering av personer och system som kommer att få åtkomst till den finansiella entitetens information. Underlåtenhet att göra detta skulle utsätta finansiella entiteter för potentiell obehörig åtkomst, dataintrång och bedräglig verksamhet och därmed äventyra konfidentialiteten, integriteten och tillgängligheten för känsliga finansiella uppgifter. Även om användningen av generiska eller delade konton undantagsvis bör tillåtas under omständigheter som specificeras av finansiella entiteter, bör finansiella entiteter säkerställa att ansvarsskyldigheten för åtgärder som vidtas via dessa konton upprätthålls. Utan denna skyddsåtgärd skulle potentiella användare med ont uppsåt kunna hindra utredningsåtgärder och korrigerande åtgärder, vilket skulle göra finansiella entiteter sårbara för oupptäckt skadlig verksamhet eller påföljder för bristande efterlevnad.

(15) För att hantera den snabba utvecklingen inom IKT-miljöer bör de finansiella entiteter som avses i avdelning II i denna förordning införa solida strategier och förfaranden för IKT-projekthantering för att upprätthålla uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet. Dessa strategier och förfaranden för IKT-projekthantering bör identifiera de delar som är nödvändiga för att framgångsrikt hantera IKT-projekt, inbegripet förändringar, förvärv, underhåll och utveckling av den finansiella entitetens IKT-system, oavsett vilken metod för IKT-projekthantering som den finansiella entiteten har valt. I samband med dessa strategier och förfaranden bör finansiella entiteter tillämpa testpraxis och testmetoder som passar deras behov, samtidigt som de följer en riskbaserad metod och säkerställer att en säker, tillförlitlig och motståndskraftig IKT-miljö upprätthålls. För att garantera ett säkert genomförande av ett IKT-projekt bör de finansiella entiteterna säkerställa att personal från specifika affärssektorer eller med roller som påverkas eller berörs av IKT-projektet kan tillhandahålla nödvändig information och expertis. För att säkerställa en effektiv tillsyn bör rapporter om IKT-projekt, särskilt om projekt som berör kritiska eller viktiga funktioner och om deras tillhörande risker, lämnas till ledningsorganet. Finansiella entiteter bör anpassa frekvensen för och inslagen i de systematiska och löpande översynerna och rapporterna till de berörda IKT-projektens betydelse och storlek.

(16) Programvarupaket som de finansiella entiteter som avses i avdelning II i denna förordning förvärvar och utvecklar måste på ett effektivt och säkert sätt integreras i den befintliga IKT-miljön, i enlighet med fastställda verksamhets- och informationssäkerhetsmål. Finansiella entiteter bör därför noggrant utvärdera sådana programvarupaket. I detta syfte, och för att identifiera sårbarheter och potentiella säkerhetsluckor inom både programvarupaket och de bredare IKT-systemen, bör finansiella entiteter utföra IKT-säkerhetstestning. För att bedöma programvarans integritet och säkerställa att användningen av den programvaran inte medför IKT-säkerhetsrisker bör finansiella entiteter också granska källkoder för förvärvad programvara, inklusive, där så är möjligt, för proprietär programvara som

tillhandahålls av tredjepartsleverantörer av IKT-tjänster, med hjälp av både statiska och dynamiska testmetoder.

(17) Förändringar, oavsett omfattning, medför inneboende risker och kan innebära betydande risker för att uppgifternas konfidentialitet, integritet och tillgänglighet förloras, och kan därmed leda till allvarliga störningar i verksamheten. För att skydda finansiella entiteter mot potentiella IKT-sårbarheter och IKT-svagheter som kan utsätta dem för betydande risker, är en strikt verifieringsprocess nödvändig för att bekräfta att alla förändringar uppfyller de nödvändiga IKT-säkerhetskraven. Finansiella entiteter som avses i avdelning II i denna förordning bör därför, som en väsentlig del av sina IKT-relaterade säkerhetsstrategier och förfaranden, införa sunda strategier och förfaranden för hantering av IKT-förändringar. För att upprätthålla objektiviteten och ändamålsenligheten i processen för hantering av IKT-förändringar, förhindra intressekonflikter och säkerställa att IKT-förändringar utvärderas objektivt, måste de funktioner som ansvarar för att godkänna dessa förändringar skiljas från de funktioner som begär och genomför dessa förändringar. För att uppnå effektiva omställningar, kontrollerat genomförande av IKT-förändringar och minimala störningar i driften av IKT-systemen bör de finansiella entiteterna fastställa tydliga roller och ansvarsområden som säkerställer att IKT-förändringar planeras och testas på lämpligt sätt och att kvaliteten säkerställs. För att säkerställa att IKT-system fortsätter att fungera effektivt, och för att tillhandahålla ett skyddsnät för finansiella entiteter, bör finansiella entiteter också utveckla och genomföra reservförfaranden. Finansiella entiteter bör tydligt identifiera dessa reservförfaranden och tilldela ansvar för att säkerställa en snabb och effektiv respons i händelse av misslyckade IKT-förändringar.

(18) För att upptäcka, hantera och rapportera IKT-relaterade incidenter bör de finansiella entiteter som avses i avdelning II i denna förordning fastställa en strategi för IKT-relaterade incidenter som omfattar komponenterna i en process för hantering av IKT-relaterade incidenter. I detta syfte bör de finansiella entiteterna identifiera alla relevanta kontakter inom och utanför organisationen som kan underlätta korrekt samordning och genomförande av de olika faserna i denna process. För att optimera upptäckten och hanteringen av IKT-relaterade incidenter och identifiera trender för sådana incidenter, som är en värdefull informationskälla som gör det möjligt för finansiella entiteter att identifiera och hantera grundorsaker och problem på ett ändamålsenligt sätt, bör finansiella entiteter särskilt detaljanalysera de IKT-relaterade incidenter som de anser vara mest betydande, bland annat eftersom de regelbundet återkommer.

(19) För att garantera en tidig och effektiv upptäckt av onormal verksamhet bör de finansiella entiteter som avses i avdelning II i denna förordning samla in, övervaka och analysera de olika informationskällorna och fördela relaterade roller och ansvarsområden. När det gäller interna informationskällor är loggar en ytterst relevant källa, men finansiella entiteter bör inte förlita sig enbart på loggar. I stället bör de finansiella entiteterna överväga att bredda informationen till att omfatta vad som rapporteras av andra interna funktioner, eftersom dessa funktioner ofta är en värdefull källa till relevant information. Av samma skäl bör finansiella entiteter analysera och övervaka information som samlats in från externa källor, inklusive information som tillhandahålls av tredjepartsleverantörer av IKT-tjänster om incidenter som berör deras system och nätverk, och andra informationskällor som finansiella entiteter anser vara relevanta. I den mån sådan information utgör personuppgifter är unionens dataskyddslagstiftning tillämplig. Personuppgifterna bör begränsas till vad som är nödvändigt för att upptäcka incidenter.

(20) För att underlätta upptäckt av IKT-relaterade incidenter bör finansiella entiteter bevara bevisning för sådana incidenter. För att å ena sidan säkerställa att sådan bevisning bevaras tillräckligt länge och å andra sidan undvika en alltför stor regelbörda, bör finansiella entiteter fastställa lagringstiden med beaktande av bland annat uppgifternas kritikalitet och lagringskrav som härrör från unionsrätten.

(21) För att säkerställa att IKT-relaterade incidenter upptäcks i tid bör de finansiella entiteter som avses i avdelning II i denna förordning betrakta de kriterier som fastställs för att utlösa processer för upptäckt och hantering av IKT-relaterade incidenter som icke uttömmande. Även om finansiella entiteter bör beakta vart och ett av dessa kriterier, bör vidare de omständigheter som beskrivs i kriterierna inte behöva inträffa samtidigt, och betydelsen av de berörda IKT-tjänsterna bör beaktas på lämpligt sätt vid utlösandet av processer för upptäckt och hantering av IKT-relaterade incidenter.

(22) När finansiella entiteter som avses i avdelning II i denna förordning utarbetar en IKT-kontinuitetspolicy bör de ta hänsyn till de väsentliga komponenterna i IKT-riskhantering, inbegripet strategier för hantering och kommunikation av IKT-relaterade incidenter, processen för hantering av IKT-förändringar och risker förknippade med tredjepartsleverantörer av IKT-tjänster.

(23) Det är nödvändigt att fastställa den uppsättning scenarier som de finansiella entiteter som avses i avdelning II i denna förordning bör beakta både vid genomförandet av åtgärds- och återställningsplaner avseende IKT och testning av IKT-kontinuitetsplaner. Dessa scenarier bör tjäna som utgångspunkt för de finansiella entiteternas analys av både relevansen och rimligheten i varje scenario och behovet av att utveckla alternativa scenarier. Finansiella entiteter bör fokusera på de scenarier där investeringar i åtgärder för motståndskraft skulle kunna vara mer effektiva och ändamålsenliga. Genom att testa byten mellan den primära IKT-infrastrukturen och reservkapacitet, säkerhetskopior och reservanläggningar bör finansiella institut bedöma om denna kapacitet och dessa säkerhetskopior och anläggningar fungerar effektivt under en tillräckligt lång tidsperiod och säkerställa att den primära IKT-infrastrukturens normala funktion återställs i enlighet med återställningsmålen.

(24) Det är nödvändigt att fastställa krav för operativ risk, och mer specifikt krav på IKT-projekthantering och hantering av IKT-förändringar samt IKT-kontinuitetshantering med utgångspunkt i de krav som redan gäller för centrala motparter, värdepapperscentraler och handelsplatser enligt Europaparlamentets och rådets förordningar (EU) nr 648/2012[4], (EU) nr 600/2014[5] och (EU) nr 909/2014[6].

(25) Enligt artikel 6.5 i förordning (EU) 2022/2554 ska finansiella entiteter se över sin IKT-riskhanteringsram och lämna en rapport om denna översyn till sin behöriga myndighet. För att de behöriga myndigheterna enkelt ska kunna behandla informationen i dessa rapporter, och för att garantera en lämplig överföring av denna

---

4 Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

5 Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

6 Europaparlamentets och rådets förordning (EU) nr 909/2014 av den 23 juli 2014 om förbättrad värdepappersavveckling i Europeiska unionen och om värdepapperscentraler samt ändring av direktiv 98/26/EG och 2014/65/EU och förordning (EU) nr 236/2012 (EUT L 257, 28.8.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

information, bör de finansiella entiteterna lämna in dessa rapporter i ett sökbart elektroniskt format.

(26) Kraven för finansiella entiteter som omfattas av den förenklade IKT-riskhanteringsram som avses i artikel 16 i förordning (EU) 2022/2554 bör inriktas på de väsentliga områden och delar som, mot bakgrund av dessa finansiella entiteters omfattning, risk, storlek och komplexitet, minst måste ingå för att säkerställa konfidentialitet, integritet, tillgänglighet och äkthet hos de finansiella entiteternas uppgifter och tjänster. I detta sammanhang bör dessa finansiella entiteter ha en intern styrnings- och kontrollram med tydliga ansvarsområden, för att möjliggöra en effektiv och sund riskhanteringsram. För att minska den administrativa och operativa bördan bör dessa finansiella entiteter dessutom utarbeta och dokumentera endast en uppsättning riktlinjer, dvs. riktlinjer för informationssäkerhet, som anger de principer och regler på hög nivå som krävs för att skydda konfidentialitet, integritet, tillgänglighet och äkthet hos dessa finansiella entiteters uppgifter och tjänster .

(27) Bestämmelserna i denna förordning avser IKT-riskhanteringsramen, genom att i detalj beskriva specifika delar som är tillämpliga på finansiella entiteter i enlighet med artikel 15 i förordning (EU) 2022/2554 och genom att utforma den förenklade IKT-riskhanteringsram för finansiella entiteter som anges i artikel 16.1 i den förordningen. För att säkerställa samstämmighet mellan den ordinarie och den förenklade IKT-riskhanteringsramen, och med tanke på att dessa bestämmelser bör bli tillämpliga samtidigt, bör dessa bestämmelser anges i en enda lagstiftningsakt.

(28) Denna förordning grundar sig på det förslag till tekniska standarder för tillsyn som lämnats till kommissionen av Europeiska bankmyndigheten, Europeiska försäkrings- och tjänstepensionsmyndigheten och Europeiska värdepappers- och marknadsmyndigheten (de europeiska tillsynsmyndigheterna), i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa).

(29) De europeiska tillsynsmyndigheternas gemensamma kommitté, som avses i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1093/2010[7], artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1094/2010[8] och artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1095/2010[9], har genomfört öppna offentliga samråd om det förslag till tekniska standarder för tillsyn som denna förordning grundar sig på, analyserat de potentiella kostnaderna för och fördelarna med de föreslagna standarderna och begärt råd från den bankintressentgrupp som inrättats i enlighet med artikel 37 i förordning (EU) nr 1093/2010, den intressentgrupp för försäkring och återförsäkring och den intressentgrupp för tjänstepensioner som inrättats i enlighet med artikel 37 i förordning (EU) nr 1094/2010 samt den

---

7 Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

8 Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

9 Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

intressentgrupp för värdepapper och marknader som inrättats i enlighet med artikel 37 i förordning (EU) nr 1095/2010.

(30) I den mån behandling av personuppgifter krävs för att fullgöra de skyldigheter som anges i denna akt bör Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 och Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 tillämpas fullt ut. Till exempel bör principen om uppgiftsminimering följas när personuppgifter samlas in för att säkerställa en lämplig upptäckt av incidenter. Europeiska datatillsynsmannen har också rådfrågats om utkastet till denna akt.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVDELNING I

ALLMÄN PRINCIP

Artikel 1
Allmän riskprofil och komplexitet

Vid utarbetande och genomförande av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i avdelning II och den förenklade IKT-riskhanteringsram som avses i avdelning III, ska hänsyn tas till den finansiella entitetens storlek och allmänna riskprofil, samt till karaktären på, omfattningen av och inslagen av ökad eller minskad komplexitet i dess tjänster, verksamhet och insatser, inbegripet delar som rör

(a) kryptering och kryptografi,

(b) säkerhet för IKT-verksamhet,

(c) nätverkssäkerhet,

(d) IKT-projekthantering och hantering av IKT-förändringar,

(e) IKT-riskens potentiella inverkan på uppgifternas konfidentialitet, integritet och tillgänglighet, och avbrottens potentiella inverkan på kontinuiteten och tillgängligheten i den finansiella entitetens verksamhet.

AVDELNING II
YTTERLIGARE HARMONISERING AV VERKTYG, METODER, PROCESSER OCH STRATEGIER FÖR IKT-RISKHANTERING I ENLIGHET MED ARTIKEL 15 I FÖRORDNING (EU) 2022/2554

KAPITEL I
IKT-RELATERADE SÄKERHETSSTRATEGIER, FÖRFARANDEN, PROTOKOLL OCH VERKTYG

AVSNITT 1

Artikel 2

Allmänna delar av IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg

1. Finansiella entiteter ska säkerställa att deras IKT-relaterade säkerhetsstrategier, informationssäkerhet och därtill hörande förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 är integrerade i deras IKT-riskhanteringsram. Finansiella entiteter ska inrätta IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg enligt detta kapitel som

   (a) säkerställer säkerheten i nätverk,

   (b) innehåller skyddsåtgärder mot intrång och missbruk av uppgifter,

   (c) bevarar uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet, inbegripet genom användning av krypteringsmetoder,

   (d) garanterar en korrekt och snabb dataöverföring utan allvarliga avbrott och onödiga dröjsmål.

2. Finansiella entiteter ska säkerställa att de IKT-relaterade säkerhetsstrategier som avses i punkt 1

   (a) är anpassade till den finansiella entitetens informationssäkerhetsmål som ingår i den strategi för digital operativ motståndskraft som avses i artikel 6.8 i förordning (EU) 2022/2554,

   (b) anger datumet för ledningsorganets formella godkännande av IKT-relaterade säkerhetsstrategier,

   (c) innehåller indikatorer och åtgärder för att

      i) övervaka genomförandet av IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg,

      ii) registrera undantag från detta genomförande,

      iii) säkerställa att den finansiella entitetens digitala operativa motståndskraft säkerställs i samband med de undantag som avses i led ii,

   (d) specificerar ansvaret för personal på alla nivåer i fråga om att säkerställa den finansiella entitetens IKT-relaterade säkerhet,

(e) anger konsekvenserna när den finansiella entitetens personal inte följer de IKT-relaterade säkerhetsstrategierna, om bestämmelser om detta inte fastställs i den finansiella entitetens övriga strategier,

(f) förtecknar den dokumentation som ska bevaras,

(g) specificerar arrangemangen för åtskillnad av arbetsuppgifter inom ramen för modellen med tre försvarslinjer eller en annan intern riskhanterings- och kontrollmodell, beroende på vad som är tillämpligt, i syfte att undvika intressekonflikter,

(h) beaktar ledande praxis och, i tillämpliga fall, standarder enligt definitionen i artikel 2.1 i förordning (EU) nr 1025/2012,

(i) identifierar roller och ansvarsområden för att utarbeta, genomföra och upprätthålla dessa IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg,

(j) ses över i enlighet med artikel 6.5 i förordning (EU) 2022/2554,

(k) tar hänsyn till väsentliga förändringar som rör den finansiella entiteten, inbegripet väsentliga förändringar i den finansiella entitetens verksamhet eller processer, i cyberhotbilden eller i tillämpliga rättsliga skyldigheter.

AVSNITT 2

Artikel 3
IKT-riskhantering

Finansiella entiteter ska utarbeta, dokumentera och genomföra strategier och förfaranden för IKT-riskhantering som ska innehålla allt av följande:

(a) En indikation på godkännandet av risktoleransnivån för IKT-risk enligt artikel 6.8 b i förordning (EU) 2022/2554.

(b) Ett förfarande och en metod för att genomföra IKT-riskbedömningen, som identifierar

i) sårbarheter och hot som berör eller kan beröra de affärsfunktioner som stöds och de IKT-system och IKT-tillgångar som stöder dessa funktioner,

ii) kvantitativa eller kvalitativa indikatorer för att mäta effekten av och sannolikheten för de sårbarheter och hot som avses i led i.

(c) Förfarandet för att identifiera, genomföra och dokumentera IKT-riskhanteringsåtgärder för de IKT-risker som identifierats och bedömts, inbegripet fastställandet av IKT-riskhanteringsåtgärder som är nödvändiga för att IKT-risken ska ligga inom den risktoleransnivå som avses i led a.

(d) När det gäller de kvarstående IKT-risker som fortfarande föreligger efter genomförandet av de IKT-riskhanteringsåtgärder som avses i led c:

i) Bestämmelser om identifiering av dessa kvarstående IKT-risker.

ii) Fördelning av roller och ansvarsområden avseende

(1) accepterandet av de kvarstående IKT-risker som överskrider den finansiella entitetens risktoleransnivå enligt led a,

(2) den översynsprocess som avses i led iv i detta led d.

iii) Utarbetandet av en förteckning av de accepterade kvarstående IKT-riskerna, inklusive en motivering till varför de accepteras.

iv) Bestämmelser om översyn av de accepterade kvarstående IKT-riskerna minst en gång per år, inbegripet

1) identifiering av eventuella förändringar av de kvarstående IKT-riskerna,

2) bedömning av tillgängliga begränsningsåtgärder,

3) bedömning av huruvida de skäl som motiverar accepterandet av kvarstående IKT-risker fortfarande är giltiga och tillämpliga vid tidpunkten för översynen.

(e) Bestämmelser om övervakning av

i) eventuella förändringar i IKT-riskbilden och cyberhotbilden,

ii) interna och externa sårbarheter och hot,

iii) den finansiella entitetens IKT-risk, vilket möjliggör snabb upptäckt av förändringar som kan beröra dess IKT-riskprofil.

(f) Bestämmelser om en process för att säkerställa att förändringar av den finansiella entitetens affärsstrategi och strategi för digital operativ motståndskraft beaktas.

Vid tillämpning av första stycket c ska det förfarande som avses i det ledet säkerställa

(a) övervakning av ändamålsenligheten hos de IKT-riskhanteringsåtgärder som genomförts,

(b) bedömning av huruvida den finansiella entitetens fastställda risktoleransnivåer har uppnåtts,

(c) bedömning av huruvida den finansiella entiteten har vidtagit åtgärder för att vid behov korrigera eller förbättra dessa åtgärder.

AVSNITT 3
HANTERING AV IKT-TILLGÅNGAR

Artikel 4
Policy för hantering av IKT-tillgångar

1. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra en policy för hantering av IKT-tillgångar.

2. Den policy för hantering av IKT-tillgångar som avses i punkt 1 ska

(a) föreskriva övervakning och hantering av livscykeln för IKT-tillgångar som identifierats och klassificerats i enlighet med artikel 8.1 i förordning (EU) 2022/2554,

(b) föreskriva att den finansiella entiteten ska föra register över

i) den unika identifieraren för varje IKT-tillgång,

ii) information om platsen, antingen fysisk eller logisk, för samtliga IKT-tillgångar,

iii) klassificeringen av samtliga IKT-tillgångar, enligt artikel 8.1 i förordning (EU) 2022/2254,

iv) identiteten hos ägare av IKT-tillgångar,

v) de affärsfunktioner eller affärstjänster som stöds av IKT-tillgången,

vi) kraven på IKT-kontinuitet, inklusive mål för återställningstid och mål för återställningspunkt,

vii) huruvida IKT-tillgången kan vara eller är exponerad mot externa nätverk, inbegripet internet,

viii) kopplingar och ömsesidiga beroenden mellan IKT-tillgångar och de affärsfunktioner som använder respektive IKT-tillgång,

ix) i tillämpliga fall och för samtliga IKT-tillgångar, slutdatum för tredjepartsleverantörens ordinarie, utökade och anpassade supporttjänster, efter vilket dessa IKT-tillgångar inte längre stöds av deras leverantör eller av en tredjepartsleverantör av IKT-tjänster,

(c) när det gäller andra finansiella entiteter än mikroföretag, föreskriva att dessa finansiella entiteter ska föra register över den information som krävs för att utföra en specifik IKT-riskbedömning av alla äldre IKT-system enligt artikel 8.7 i förordning (EU) 2022/2554.

Artikel 5
Förfarande för hantering av IKT-tillgångar

1. Finansiella entiteter ska utarbeta, dokumentera och genomföra ett förfarande för hantering av IKT-tillgångar.

2. Det förfarande för hantering av IKT-tillgångar som avses i punkt 1 ska ange kriterierna för att utföra en bedömning av kritikaliteten hos informationstillgångar och IKT-tillgångar som stöder affärsfunktioner. Denna bedömning ska ta hänsyn till

(a) den IKT-risk som är kopplad till dessa affärsfunktioner och deras beroende av informationstillgångarna eller IKT-tillgångarna,

(b) hur en förlust av konfidentialitet, integritet och tillgänglighet för sådana informationstillgångar och IKT-tillgångar skulle påverka de finansiella entiteternas affärsprocesser och verksamhet.

AVSNITT 4
KRYPTERING OCH KRYPTOGRAFI

Artikel 6
Kryptering och kryptografisk säkerhet

1. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra en policy för kryptering och kryptografisk säkerhet.

2. Finansiella entiteter ska utforma den policy för kryptering och kryptografisk säkerhet som avses i punkt 1 på grundval av resultaten av en godkänd dataklassificering och IKT-riskbedömning. Denna policy ska innehålla regler för

(a) kryptering av uppgifter i vila och under överföring,

(b) kryptering av uppgifter i bruk, vid behov,

(c) kryptering av interna nätverksanslutningar och trafik med externa parter,

(d) den hantering av kryptografiska nycklar som avses i artikel 7, med fastställande av regler för korrekt användning, skydd och livscykel i fråga om kryptografiska nycklar.

Vid tillämpning av led b ska finansiella entiteter, om kryptering av uppgifter i bruk inte är möjlig, behandla uppgifter i bruk i en avskild och skyddad miljö, eller vidta likvärdiga åtgärder för att säkerställa uppgifternas konfidentialitet, integritet, äkthet och tillgänglighet.

3. Finansiella entiteter ska i den policy för kryptering och kryptografisk säkerhet som avses i punkt 1 inkludera kriterier för val av krypteringsmetoder och användningspraxis, med beaktande av ledande praxis och standarder enligt definitionen i artikel 2.1 i förordning (EU) nr 1025/2012, och den klassificering av relevanta IKT-tillgångar som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554. Finansiella entiteter som inte kan följa ledande praxis eller standarder, eller använda de mest tillförlitliga metoderna, ska anta begränsnings- och övervakningsåtgärder som säkerställer motståndskraft mot cyberhot.

4. Finansiella entiteter ska i den policy för kryptering och kryptografisk säkerhet som avses i punkt 1 inkludera bestämmelser om uppdatering eller ändring, vid behov, av krypteringstekniken på grundval av utvecklingen inom kryptoanalys. Dessa uppdateringar eller ändringar ska säkerställa att krypteringstekniken förblir motståndskraftig mot cyberhot, i enlighet med artikel 10.2 a. Finansiella entiteter som inte kan uppdatera eller ändra krypteringstekniken ska anta begränsnings- och övervakningsåtgärder som säkerställer motståndskraft mot cyberhot.

5. Finansiella entiteter ska i den policy för kryptering och kryptografisk säkerhet som avses i punkt 1 inkludera ett krav på att dokumentera antagandet av begränsnings- och övervakningsåtgärder som antagits i enlighet med punkterna 3 och 4 och att ge en motiverad förklaring till detta.

Artikel 7
Hantering av kryptografiska nycklar

1. Finansiella entiteter ska i den policy för hantering av kryptografiska nycklar som avses i artikel 6.2 d inkludera krav för hantering av kryptografiska nycklar under hela deras livscykel, inbegripet generering, förnyelse, lagring, säkerhetskopiering, arkivering, hämtning, överföring, återkallande, upphävande och förstörelse av dessa kryptografiska nycklar.

2. Finansiella entiteter ska identifiera och genomföra kontroller för att skydda kryptografiska nycklar under hela deras livscykel mot förlust, obehörig åtkomst, röjande och ändring. Finansiella entiteter ska utforma dessa kontroller på grundval av resultaten av den godkända dataklassificeringen och IKT-riskbedömningen.

3. Finansiella entiteter ska utveckla och genomföra metoder för att ersätta kryptografiska nycklar i händelse av förlust, eller om dessa nycklar är komprometterade eller skadade.

4. Finansiella entiteter ska skapa och upprätthålla ett register över alla certifikat och enheter för lagring av certifikat för åtminstone IKT-tillgångar som stöder kritiska eller viktiga funktioner. Finansiella entiteter ska hålla detta register uppdaterat.

5. Finansiella entiteter ska säkerställa att certifikat snabbt förnyas innan de löper ut.

AVSNITT 5
SÄKERHET FÖR IKT-VERKSAMHET

Artikel 8
Strategier och förfaranden för IKT-verksamhet

1. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra strategier och förfaranden för hantering av IKT-verksamheten. Dessa strategier och förfaranden ska specificera hur finansiella entiteter driver, övervakar, kontrollerar och återställer sina IKT-tillgångar, inbegripet dokumentation av IKT-verksamhet.

2. De strategier och förfaranden för IKT-verksamhet som avses i punkt 1 ska innehålla allt av följande:

   (a) En beskrivning av IKT-tillgångarna, inklusive

      i) krav avseende säker installation, säkert underhåll och säker konfiguration och avinstallation av ett IKT-system,

      ii) krav avseende hantering av informationstillgångar som används av IKT-tillgångar, däribland deras bearbetning och hantering och både automatiserad och manuell sådan,

      iii) krav avseende identifiering och kontroll av äldre IKT-system.

   (b) Kontroll och övervakning av IKT-system, inklusive

      i) krav på säkerhetskopiering och återställning av IKT-system,

      ii) krav på schemaläggning, med beaktande av ömsesidiga beroenden mellan IKT-systemen,

      iii) protokoll för revisionsloggning och systemlogginformation,

      iv) krav för att säkerställa att utförandet av internrevision och annan testning minimerar störningar i affärsverksamheten,

      v) krav på separering av IKT-produktionsmiljöer från utvecklingsmiljöer, testmiljöer och andra miljöer som inte är produktionsmiljöer,

      vi) krav på att genomföra utveckling och testning i miljöer som är åtskilda från produktionsmiljön,

      vii) krav på att genomföra utveckling och testning i produktionsmiljöer.

   (c) Felhantering avseende IKT-system, inklusive

      i) förfaranden och protokoll för felhantering,

      ii) kontakter för support och eskalering, inklusive externa supportkontakter i händelse av oväntade operativa eller tekniska problem,

      iii) förfaranden för omstart, återladdning och återställning av IKT-system för användning i händelse av avbrott i IKT-system.

   Vid tillämpning av led b v ska separeringen beakta alla komponenter i miljön, inbegripet konton, uppgifter eller anslutningar, enligt artikel 13.1 a.

Vid tillämpning av led b vii ska de strategier och förfaranden som avses i punkt 1 föreskriva att de fall då testning utförs i en produktionsmiljö är tydligt identifierade, motiverade, gäller begränsade tidsperioder och är godkända av den relevanta funktionen i enlighet med artikel 16.6. Finansiella entiteter ska säkerställa tillgänglighet, konfidentialitet, integritet och äkthet för IKT-system och produktionsdata under utveckling och testning i produktionsmiljön.

Artikel 9
Kapacitets- och prestandahantering

1. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra förfaranden för kapacitets- och prestandahantering när det gäller följande:

   (a) Identifiering av kapacitetskrav för deras IKT-system.

   (b) Tillämpning av resursoptimering.

   (c) Övervakningsförfaranden för att upprätthålla och förbättra

      i) tillgängligheten till uppgifter och IKT-system,

      ii) IKT-systemens effektivitet,

      iii) förebyggande av brist på IKT-kapacitet.

2. De förfaranden för kapacitets- och prestandahantering som avses i punkt 1 ska säkerställa att finansiella entiteter vidtar lämpliga åtgärder för att beakta särdragen hos IKT-system med långa eller komplexa upphandlings- eller godkännandeförfaranden eller hos IKT-system som är resursintensiva.

Artikel 10
Hantering av sårbarheter och programfixar

1. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra förfaranden för sårbarhetshantering.

2. De förfaranden för sårbarhetshantering som avses i punkt 1 ska

   (a) identifiera och uppdatera relevanta och tillförlitliga informationsresurser för att bygga upp och upprätthålla medvetenheten om sårbarheter,

   (b) säkerställa utförandet av automatiserade sårbarhetsbedömningar och bedömningar av IKT-tillgångar, varvid frekvensen för och omfattningen av dessa aktiviteter ska stå i proportion till den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554 och IKT-tillgångens allmänna riskprofil,

   (c) kontrollera huruvida

      i) tredjepartsleverantörer av IKT-tjänster hanterar sårbarheter relaterade till de IKT-tjänster som tillhandahålls den finansiella entiteten,

      ii) dessa tjänsteleverantörer i god tid rapporterar till den finansiella entiteten åtminstone de kritiska sårbarheterna och statistik och trender,

   (d) spåra användningen av

i) tredjepartsbibliotek, inklusive bibliotek med öppen källkod, som används av IKT-tjänster som stöder kritiska eller viktiga funktioner,

ii) IKT-tjänster som utvecklats av den finansiella entiteten själv eller som specifikt anpassats eller utvecklats för den finansiella entiteten av en tredjepartsleverantör av IKT-tjänster,

(e) upprätta förfaranden för ansvarsfullt offentliggörande av sårbarheter till kunder, motparter och till allmänheten,

(f) prioritera införandet av programfixar och andra begränsningsåtgärder för att hantera de identifierade sårbarheterna,

(g) övervaka och kontrollera avhjälpandet av sårbarheter,

(h) kräva registrering av alla upptäckta sårbarheter som berör IKT-system och övervakning av hur de åtgärdas.

Vid tillämpning av led b ska finansiella entiteter utföra automatiserade sårbarhetsbedömningar och bedömningar av IKT-tillgångar för de IKT-tillgångar som stöder kritiska eller viktiga funktioner minst en gång i veckan.

Vid tillämpning av led c ska finansiella entiteter begära att tredjepartsleverantörer av IKT-tjänster undersöker de relevanta sårbarheterna, fastställer grundorsakerna och genomför lämpliga begränsningsåtgärder.

Vid tillämpning av led d ska finansiella entiteter, när så är lämpligt i samarbete med tredjepartsleverantören av IKT-tjänster, övervaka versionen och potentiella uppdateringar av tredjepartsbiblioteken. När det gäller IKT-tillgångar som är färdiga att använda (från lager) eller delar av IKT-tillgångar som förvärvats och används för IKT-tjänster som inte stöder kritiska eller viktiga funktioner, ska finansiella entiteter i möjligaste mån spåra användningen av tredjepartsbibliotek, inklusive bibliotek med öppen källkod.

Vid tillämpning av led f ska finansiella entiteter beakta sårbarhetens kritikalitet, den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554 och riskprofilen för de IKT-tillgångar som berörs av de identifierade sårbarheterna.

3. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra förfaranden för hantering av programfixar.

4. De förfaranden för hantering av programfixar som avses i punkt 3 ska

(a) i möjligaste mån identifiera och utvärdera tillgängliga program- och hårdvarufixar och program- och hårdvaruuppdateringar med hjälp av automatiserade verktyg,

(b) identifiera nödförfaranden för fixning och uppdatering av IKT-tillgångar,

(c) testa och införa de program- och hårdvarufixar och de program- och hårdvaruuppdateringar som avses i artikel 8.2 b v, vi och vii,

(d) fastställa tidsfrister för installation av program- och hårdvarufixar och program- och hårdvaruuppdateringar samt eskaleringsförfaranden om dessa tidsfrister inte kan hållas.

Artikel 11
Data- och systemsäkerhet

1. Som en del av de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i förordning (EU) 2022/2554 ska finansiella entiteter utarbeta, dokumentera och genomföra ett förfarande för data- och systemsäkerhet.

2. Det förfarande för data- och systemsäkerhet som avses i punkt 1 ska innehålla samtliga följande delar som rör data- och IKT-systemsäkerhet, i enlighet med den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554:

   (a) De åtkomstbegränsningar som avses i artikel 21 i den här förordningen och som stöder skyddskraven för varje klassificeringsnivå.

   (b) Identifiering av en baslinje för säker konfiguration för IKT-tillgångar vilken minimerar dessa IKT-tillgångars exponering för cyberhot, och åtgärder för att regelbundet kontrollera att dessa baslinjer används ändamålsenligt.

   (c) Identifiering av säkerhetsåtgärder för att säkerställa att endast godkänd programvara installeras i IKT-system och slutpunktsenheter.

   (d) Identifiering av säkerhetsåtgärder mot skadlig kod.

   (e) Identifiering av säkerhetsåtgärder för att säkerställa att endast godkända datalagringsmedier, system och slutpunktsenheter används för att överföra och lagra uppgifter från den finansiella entiteten.

   (f) Följande krav för att säkra användningen av bärbara slutpunktsenheter och privata icke-bärbara slutpunktsenheter:

      i) Kravet att använda en hanteringslösning för att fjärrhantera slutpunktsenheterna och fjärrensa den finansiella entitetens uppgifter.

      ii) Kravet att använda säkerhetsmekanismer som inte kan ändras, tas bort eller kringgås av personal eller tredjepartsleverantörer av IKT-tjänster på ett obehörigt sätt.

      iii) Kravet att använda flyttbara datalagringsenheter endast om den kvarstående IKT-risken ligger inom den finansiella entitetens risktoleransnivå enligt artikel 3 första stycket a.

   (g) Processen för att på ett säkert sätt radera uppgifter som finns i den finansiella entitetens lokaler eller lagras externt, och som den finansiella entiteten inte längre behöver samla in eller lagra.

   (h) Processen för att på ett säkert sätt bortskaffa eller obrukbargöra datalagringsenheter som finns i den finansiella entitetens lokaler eller lagras externt, och som innehåller konfidentiell information.

   (i) Identifiering och genomförande av säkerhetsåtgärder för att förhindra dataförlust och dataläckage för system och slutpunktsenheter.

   (j) Genomförande av säkerhetsåtgärder för att säkerställa att distansarbete och användning av privata slutpunktsenheter inte negativt påverkar den finansiella entitetens IKT-säkerhet.

   (k) När det gäller IKT-tillgångar eller tjänster som tillhandahålls av en tredjepartsleverantör av IKT-tjänster, identifiering och genomförande av krav för att upprätthålla digital operativ motståndskraft, i enlighet med resultaten av dataklassificeringen och IKT-riskbedömningen.

Vid tillämpning av led b ska den baslinje för säker konfiguration som avses i det ledet beakta ledande praxis och lämpliga metoder som fastställs i de standarder som definieras i artikel 2.1 i förordning (EU) nr 1025/2012.

Vid tillämpning av led k ska finansiella entiteter beakta följande:

(a) Genomförande av leverantörens rekommenderade inställningar på de delar som används av den finansiella entiteten.

(b) En tydlig fördelning av roller och ansvarsområden för informationssäkerhet mellan den finansiella entiteten och tredjepartsleverantören av IKT-tjänster, i enlighet med principen om den finansiella entitetens fulla ansvar för sin tredjepartsleverantör av IKT-tjänster enligt artikel 28.1 a i förordning (EU) 2022/2554, och för finansiella entiteter som avses i artikel 28.2 i den förordningen, i enlighet med den finansiella entitetens policy för användning av IKT-tjänster som stöder kritiska eller viktiga funktioner.

(c) Behovet av att säkerställa och upprätthålla lämplig kompetens inom den finansiella entiteten när det gäller hantering av och säkerhet för den tjänst som används.

(d) Tekniska och organisatoriska åtgärder för att minimera riskerna i samband med den infrastruktur som används av tredjepartsleverantören av IKT-tjänster för dess IKT-tjänster, med beaktande av ledande praxis och standarder enligt definitionen i artikel 2.1 i förordning (EU) nr 1025/2012.

Artikel 12
Loggning

1. Finansiella entiteter ska, som en del av skyddsåtgärderna mot intrång och missbruk av uppgifter, utarbeta, dokumentera och införa förfaranden, protokoll och verktyg för loggning.

2. De förfaranden, protokoll och verktyg för loggning som avses i punkt 1 ska innehålla allt av följande:

(a) Identifiering av de händelser som ska loggas, loggarnas lagringstid och åtgärder för att säkra och hantera logguppgifterna, med beaktande av det syfte för vilket loggarna skapas.

(b) Anpassning av loggarnas detaljnivå till deras syfte och användning, för att möjliggöra effektiv upptäckt av onormal verksamhet enligt artikel 24.

(c) Kravet att logga händelser som är relaterade till

i) logisk och fysisk åtkomstkontroll, enligt artikel 21, och identitetshantering,

ii) kapacitetshantering,

iii) hantering av förändringar,

iv) IKT-verksamhet, inbegripet IKT-systemverksamhet,

v) nätverkstrafik, inbegripet IKT-nätverkens prestanda.

(d) Åtgärder för att skydda loggningssystem och logginformation mot manipulering, radering och obehörig åtkomst i vila, under överföring och, i relevanta fall, i bruk.

(e) Åtgärder för att upptäcka fel i loggningssystem.

(f) Utan att det påverkar tillämpningen av eventuella tillämpliga lagstadgade krav enligt unionsrätten eller nationell rätt, synkronisering av klockorna i den finansiella entitetens samtliga IKT-system med en dokumenterad tillförlitlig referenstidskälla.

Vid tillämpning av led a ska finansiella entiteter fastställa lagringstiden med beaktande av verksamhets- och informationssäkerhetsmålen, skälet till att händelsen registreras i loggarna och resultaten av IKT-riskbedömningen.

AVSNITT 6
NÄTVERKSSÄKERHET

Artikel 13
Hantering av nätverkssäkerhet

1. Finansiella entiteter ska, som en del av de skyddsåtgärder som säkerställer nätverkens säkerhet mot intrång och missbruk av uppgifter, utarbeta, dokumentera och införa strategier, förfaranden, protokoll och verktyg för hantering av nätverkssäkerhet, inklusive allt av följande:

(a) Segregering och segmentering av IKT-system och nätverk med beaktande av

i) kritikaliteten hos eller vikten av den funktion som dessa IKT-system och nätverk stöder,

ii) den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554,

iii) den allmänna riskprofilen för IKT-tillgångar som använder dessa IKT-system och nätverk.

(b) Dokumentation av den finansiella entitetens samtliga nätverksanslutningar och dataflöden.

(c) Användning av ett separat och särskilt nätverk för administration av IKT-tillgångar.

(d) Identifiering och genomförande av kontroller för nätverksåtkomst för att förhindra och upptäcka anslutningar till den finansiella entitetens nätverk av en obehörig enhet eller ett obehörigt system, eller någon slutpunkt som inte uppfyller den finansiella entitetens säkerhetskrav.

(e) Kryptering av nätverksanslutningar som går via företagsnätverk, offentliga nätverk, inhemska nätverk, tredje parts nätverk och trådlösa nätverk, för kommunikationsprotokoll som används, med beaktande av resultaten av den godkända dataklassificeringen, resultaten av IKT-riskbedömningen och den kryptering av nätverksanslutningar som avses i artikel 6.2.

(f) Utformning av nätverk i linje med de IKT-säkerhetskrav som fastställts av den finansiella entiteten, med beaktande av ledande praxis för att säkerställa nätverkets konfidentialitet, integritet och tillgänglighet.

(g) Säkring av nätverkstrafik mellan de interna nätverken och internet och andra externa anslutningar.

(h) Identifiering av roller och ansvarsområden samt steg för specifikation, införande, godkännande, ändring och granskning av brandväggsregler och anslutningsfilter.

(i) Granskning av nätverksarkitekturen och utformningen av nätverkssäkerheten en gång per år, och regelbundet för mikroföretag, för att identifiera potentiella sårbarheter.

(j) Åtgärder för att vid behov tillfälligt isolera delnätverk samt nätverkskomponenter och nätverksenheter.

(k) Införande av en baslinje för säker konfiguration av alla nätverkskomponenter och härdning av nätverket och nätverksenheter i linje med eventuella leverantörsanvisningar, i tillämpliga fall standarder enligt definitionen i artikel 2.1 i förordning (EU) nr 1025/2012 och ledande praxis.

(l) Förfaranden för att begränsa, låsa och avsluta system- och fjärrsessioner efter en angiven period av inaktivitet.

(m) När det gäller avtal om nätverkstjänster,

i) identifiering och specificering av IKT-säkerhetsåtgärder och informationssäkerhetsåtgärder, servicenivåer och hanteringskrav för alla nätverkstjänster,

ii) huruvida dessa tjänster tillhandahålls av en koncernintern IKT-tjänteleverantör eller av tredjepartsleverantörer av IKT-tjänster.

Vid tillämpning av led h ska finansiella entiteter regelbundet granska brandväggsregler och anslutningsfilter i enlighet med den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554 och den allmänna riskprofilen för de berörda IKT-systemen. När det gäller IKT-system som stöder kritiska eller viktiga funktioner ska finansiella entiteter kontrollera att de befintliga brandväggsreglerna och anslutningsfiltren är tillräckliga minst var sjätte månad.

Artikel 14
Säkring av information under överföring

1. Som en del av skyddsåtgärderna för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet ska de finansiella entiteterna utarbeta, dokumentera och införa strategier, förfaranden, protokoll och verktyg för att skydda information under överföring. Finansiella entiteter ska särskilt säkerställa

(a) tillgänglighet, äkthet, integritet och konfidentialitet för uppgifter under överföring i nätverk, och inrättande av förfaranden för att bedöma efterlevnaden av dessa krav,

(b) förebyggande och upptäckt av dataläckage och säker överföring av information mellan den finansiella entiteten och externa parter,

(c) att krav på konfidentialitet eller tystnadsplikt som återspeglar den finansiella entitetens behov av skydd av information för både den finansiella entitetens och tredje parts personal införs, dokumenteras och regelbundet ses över.

2. Finansiella entiteter ska utforma strategier, förfaranden, protokoll och verktyg för att skydda den information under överföring som avses i punkt 1 på grundval av resultaten av den godkända dataklassificeringen och IKT-riskbedömningen.

AVSNITT 7
IKT-PROJEKTHANTERING OCH HANTERING AV IKT-FÖRÄNDRINGAR

Artikel 15
IKT-projekthantering

1. Som en del av skyddsåtgärderna för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet ska finansiella entiteter utarbeta, dokumentera och genomföra en policy för IKT-projekthantering.

2. Den policy för IKT-projekthantering som avses i punkt 1 ska ange de delar som säkerställer en ändamålsenlig IKT-projekthantering i samband med förvärv, underhåll och, i tillämpliga fall, utveckling av den finansiella entitetens IKT-system.

3. Den policy för IKT-projekthantering som avses i punkt 1 ska innehålla allt av följande:

   (a) IKT-projektets mål.

   (b) IKT-projektets styrning, inklusive roller och ansvarsområden.

   (c) IKT-projektets planering, tidsram och steg.

   (d) Riskbedömning av IKT-projektet.

   (e) Relevanta delmål.

   (f) Krav på förändringshantering.

   (g) Testning av alla krav, inklusive säkerhetskrav, och respektive godkännandeprocess vid införande av ett IKT-system i produktionsmiljön.

4. Den policy för IKT-projekthantering som avses i punkt 1 ska säkerställa ett säkert genomförande av IKT-projekt genom tillhandahållande av nödvändig information och expertis från det affärsområde eller de funktioner som påverkas av IKT-projektet.

5. I enlighet med den riskbedömning av IKT-projekt som avses i punkt 3 d ska den policy för IKT-projekthantering som avses i punkt 1 föreskriva att inrättandet och utvecklingen av IKT-projekt som påverkar den finansiella entitetens kritiska eller viktiga funktioner och tillhörande risker rapporteras till ledningsorganet enligt följande:

   (a) Individuellt eller i aggregerad form, beroende på IKT-projektens betydelse och storlek.

   (b) Regelbundet och, vid behov, händelsebaserat.

Artikel 16
Förvärv, utveckling och underhåll av IKT-system

1. Som en del av skyddsåtgärderna för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet ska de finansiella entiteterna utarbeta, dokumentera och genomföra en policy som styr förvärv, utveckling och underhåll av IKT-system. Denna policy ska

   (a) identifiera säkerhetsrutiner och metoder som rör förvärv, utveckling och underhåll av IKT-system,

(b) kräva identifiering av

i) tekniska specifikationer och tekniska specifikationer på IKT-området, enligt definitionerna i artikel 2.4 och 2.5 i förordning (EU) nr 1025/2012,

ii) krav som rör förvärv, utveckling och underhåll av IKT-system, med särskilt fokus på IKT-säkerhetskrav och på deras godkännande av den relevanta affärsfunktionen och ägaren av IKT-tillgångar i enlighet med den finansiella entitetens interna styrningsarrangemang,

(c) specificera åtgärder för att minska risken för oavsiktlig ändring eller avsiktlig manipulering av IKT-systemen under utveckling, underhåll och införande av dessa IKT-system i produktionsmiljön.

2. Finansiella entiteter ska utarbeta, dokumentera och genomföra ett förfarande för förvärv, utveckling och underhåll av IKT-system för testning och godkännande av alla IKT-system före användning och efter underhåll, i enlighet med artikel 8.2 b v, vi och vii. Testnivån ska stå i proportion till hur kritiska de berörda affärsförfarandena och IKT-tillgångarna är. Testningen ska utformas för att verifiera att nya IKT-system är lämpliga för att fungera som avsett, inbegripet kvaliteten på den programvara som utvecklats internt.

Centrala motparter ska, utöver de krav som fastställs i första stycket, vid behov involvera följande i utformningen och genomförandet av de tester som avses i första stycket:

(a) Clearingmedlemmar och clearingkunder.

(b) Interoperabla centrala motparter.

(c) Andra berörda parter.

Värdepapperscentraler ska, utöver de krav som fastställs i första stycket, vid behov involvera följande i utformningen och genomförandet av de tester som avses i första stycket:

(a) Användare.

(b) Kritiska försörjningstjänster och kritiska tjänsteleverantörer.

(c) Andra värdepapperscentraler.

(d) Andra marknadsinfrastrukturer.

(e) Alla andra institut med vilka värdepapperscentralerna har identifierat ömsesidiga beroenden i sin kontinuitetspolicy.

3. Det förfarande som avses i punkt 2 ska omfatta granskningar av källkod som omfattar både statisk och dynamisk testning. Denna testning ska innehålla säkerhetstestning för internetexponerade system och applikationer i enlighet med artikel 8.2 b v, vi och vii. De finansiella entiteterna ska

(a) identifiera och analysera sårbarheter och avvikelser i källkoden,

(b) anta en handlingsplan för att åtgärda dessa sårbarheter och avvikelser,

(c) övervaka genomförandet av denna handlingsplan.

4. Det förfarande som avses i punkt 2 ska omfatta säkerhetstestning av programvarupaket senast i integrationsfasen, i enlighet med artikel 8.2 b v, vi och vii.

5. Det förfarande som avses i punkt 2 ska föreskriva att

(a) miljöer som inte är produktionsmiljöer endast lagrar anonymiserade, pseudonymiserade eller randomiserade produktionsdata,

(b) finansiella entiteter ska skydda uppgifternas integritet och konfidentialitet i miljöer som inte är produktionsmiljöer.

6. Genom undantag från punkt 5 får det förfarande som avses i punkt 2 föreskriva att produktionsdata lagras endast för specifika testtillfällen, under begränsade tidsperioder och efter godkännande av den relevanta funktionen och rapportering av sådana tillfällen till IKT-riskhanteringsfunktionen.

7. Det förfarande som avses i punkt 2 ska omfatta genomförandet av kontroller för att skydda integriteten hos källkoden för IKT-system som utvecklas internt eller av en tredjepartsleverantör av IKT-tjänster och som levereras till den finansiella entiteten av en tredjepartsleverantör av IKT-tjänster.

8. Det förfarande som avses i punkt 2 ska föreskriva att proprietär programvara och, om möjligt, den källkod som tillhandahålls av tredjepartsleverantörer av IKT-tjänster eller som kommer från projekt med öppen källkod ska analyseras och testas i enlighet med punkt 3 innan de införs i produktionsmiljön.

9. Punkterna 1–8 i denna artikel ska också tillämpas på IKT-system som utvecklas eller förvaltas av användare utanför IKT-funktionen, med hjälp av en riskbaserad metod.

Artikel 17
Hantering av IKT-förändringar

1. Som en del av skyddsåtgärderna för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet ska finansiella entiteter i de förfaranden för hantering av IKT-förändringar som avses i artikel 9.4 e i förordning (EU) 2022/2554, när det gäller alla ändringar av programvara, hårdvara, komponenter i fast programvara, system eller säkerhetsparametrar, inkludera samtliga följande delar:

(a) En kontroll av huruvida IKT-säkerhetskraven har uppfyllts.

(b) Mekanismer för att säkerställa oberoendet mellan de funktioner som godkänner förändringar och de funktioner som ansvarar för att begära och genomföra dessa förändringar.

(c) En tydlig beskrivning av roller och ansvarsområden för att säkerställa att

i) förändringar specificeras och planeras,

ii) en lämplig övergång utformas,

iii) förändringarna testas och slutförs på ett kontrollerat sätt,

iv) det finns en effektiv kvalitetssäkring.

(d) Dokumentation och kommunikation av uppgifter om förändringar, inklusive

i) förändringens syfte och omfattning,

ii) tidslinjen för genomförandet av förändringen,

iii) de förväntade resultaten.

(e) Identifiering av reservförfaranden och ansvarsområden för sådana, inklusive förfaranden och ansvarsområden för att avbryta förändringar eller återställa förändringar som inte genomförts framgångsrikt.

(f) Förfaranden, protokoll och verktyg för hantering av akuta förändringar som innehåller tillräckliga skyddsåtgärder.

(g) Förfaranden för att dokumentera, omvärdera, bedöma och godkänna akuta förändringar efter deras genomförande, inklusive kringgående operationer och programfixar.

(h) Identifiering av den potentiella inverkan av en förändring på befintliga IKT-säkerhetsåtgärder och en bedömning av huruvida en sådan förändring kräver att ytterligare IKT-säkerhetsåtgärder vidtas.

2. Efter att ha gjort betydande förändringar i sina IKT-system ska centrala motparter och värdepapperscentraler låta sina IKT-system genomgå stränga tester genom att simulera ansträngda lägen.

Centrala motparter ska vid behov involvera följande i utformningen och genomförandet av de tester som avses i första stycket:

(a) Clearingmedlemmar och clearingkunder.

(b) Interoperabla centrala motparter.

(c) Andra berörda parter.

Värdepapperscentraler ska vid behov involvera följande i utformningen och genomförandet av de tester som avses i första stycket:

(a) Användare.

(b) Kritiska försörjningstjänster och kritiska tjänsteleverantörer.

(c) Andra värdepapperscentraler.

(d) Andra marknadsinfrastrukturer.

(e) Alla andra institut med vilka värdepapperscentralerna har identifierat ömsesidiga beroenden i sin IKT-kontinuitetspolicy.

AVSNITT 8

Artikel 18
Fysisk säkerhet och miljösäkerhet

1. Som en del av skyddsåtgärderna för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet ska finansiella entiteter specificera, dokumentera och genomföra en policy för fysisk säkerhet och miljösäkerhet. Finansiella entiteter ska utforma denna policy mot bakgrund av cyberhotbilden, i enlighet med den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554 och mot bakgrund av den allmänna riskprofilen för IKT-tillgångar och tillgängliga informationstillgångar.

2. Den policy för fysisk säkerhet och miljösäkerhet som avses i punkt 1 ska innehålla allt av följande:

(a) En hänvisning till avsnittet i policyn om kontroll av rättigheter till åtkomsthantering som avses i artikel 21 första stycket g.

(b) Åtgärder för att skydda den finansiella entitetens lokaler, datacentraler och känsliga angivna områden som identifierats av den finansiella entiteten, där

IKT-tillgångar och informationstillgångar finns, mot angrepp, olyckor samt miljöhot och miljöfaror.

(c) Åtgärder för att säkra IKT-tillgångar, både inom och utanför den finansiella entitetens lokaler, med beaktande av resultaten av IKT-riskbedömningen för de relevanta IKT-tillgångarna.

(d) Åtgärder för att säkerställa tillgänglighet, äkthet, integritet och konfidentialitet för den finansiella entitetens IKT-tillgångar, informationstillgångar och enheter för fysisk åtkomstkontroll genom lämpligt underhåll.

(e) Åtgärder för att bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet, inklusive

i) en policy om ett renstädat skrivbord för dokument,

ii) en policy om en tom bildskärm för anläggningar för informationsbehandling.

Vid tillämpning av led b ska åtgärderna för skydd mot miljöhot och miljöfaror stå i proportion till hur viktiga lokalerna, datacentralerna och de känsliga angivna områdena är och hur kritiska de verksamheter eller IKT-system som finns där är.

Vid tillämpning av led c ska den policy för fysisk säkerhet och miljösäkerhet som avses i punkt 1 innehålla åtgärder för att tillhandahålla lämpligt skydd för obevakade IKT-tillgångar.

Kapitel II
PERSONALPOLITIK OCH ÅTKOMSTKONTROLL

Artikel 19
Personalpolitik

Finansiella entiteter ska i sin personalpolitik eller andra relevanta policyer inkludera alla följande IKT-säkerhetsrelaterade delar:

(a) Identifiering och fördelning av alla specifika ansvarsområden för IKT-säkerhet.

(b) Krav för personal hos den finansiella entiteten och hos tredjepartsleverantörer av IKT-tjänster som använder eller har åtkomst till den finansiella entitetens IKT-tillgångar att

i) vara informerad om, och följa, den finansiella entitetens IKT-relaterade säkerhetsstrategier, förfaranden och protokoll,

ii) vara medveten om de rapporteringskanaler som inrättats av den finansiella entiteten för att upptäcka onormalt beteende, inklusive, i tillämpliga fall, de rapporteringskanaler som inrättats i linje med Europaparlamentets och rådets direktiv (EU) 2019/1937[10],

iii) när anställningen upphör, till den finansiella entiteten återlämna alla IKT-tillgångar och materiella informationstillgångar som den innehar och som tillhör den finansiella entiteten.

[10] Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten (EUT L 305, 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj)

Artikel 20
Identitetshantering

1. Som en del av sin kontroll av rättigheter till åtkomsthantering ska finansiella entiteter utarbeta, dokumentera och genomföra strategier och förfaranden för identitetshantering som säkerställer unik identifiering och autentisering av fysiska personer och system som har åtkomst till den finansiella entitetens information, i syfte att möjliggöra tilldelning av åtkomsträttigheter för användare i enlighet med artikel 21.

2. De strategier och förfaranden för identitetshantering som avses i punkt 1 ska innehålla allt av följande:

   (a) Utan att det påverkar tillämpningen av artikel 21 första stycket c, en unik identitet som motsvarar ett unikt användarkonto och som tilldelas varje anställd i den finansiella entiteten eller varje anställd hos tredjepartsleverantörer av IKT-tjänster som har åtkomst till den finansiella entitetens informationstillgångar och IKT-tillgångar.

   (b) En process för livscykelhantering av identiteter och konton som hanterar skapande, ändring, granskning och uppdatering, tillfällig inaktivering och avslutande av alla konton.

   Vid tillämpning av led a ska finansiella entiteter föra register över alla identitetstilldelningar. Dessa register ska bevaras efter en omorganisation av den finansiella entiteten eller efter det att avtalsförhållandet har upphört, utan att det påverkar de krav på bevarande som fastställs i tillämplig unionsrätt och nationell rätt.

   Vid tillämpning av led b ska finansiella entiteter, när så är möjligt och lämpligt, införa automatiserade lösningar för processen för livscykelhantering av identiteter.

Artikel 21
Åtkomstkontroll

Som en del av sin kontroll av rättigheter till åtkomsthantering ska finansiella entiteter utarbeta, dokumentera och genomföra en policy som innehåller allt av följande:

(a) Tilldelning av åtkomsträttigheter till IKT-tillgångar baserat på principerna om behovsenlig behörighet, behovsenlig användning och minsta möjliga behörighet, inklusive för fjärråtkomst och nödåtkomst.

(b) Åtskillnad av arbetsuppgifter för att förhindra omotiverad åtkomst till kritiska uppgifter eller för att förhindra tilldelning av kombinationer av åtkomsträttigheter som kan användas för att kringgå kontroller.

(c) En bestämmelse om användares ansvarsskyldighet, genom att i möjligaste mån begränsa användningen av generiska och delade användarkonton och säkerställa att användarna alltid kan identifieras när åtgärder utförs i IKT-systemen.

(d) En bestämmelse om begränsningar av åtkomst till IKT-tillgångar, med angivande av kontroller och verktyg för att förhindra obehörig åtkomst.

(e) Förfaranden för kontohantering för att bevilja, ändra eller återkalla åtkomsträttigheter för användarkonton och generiska konton, även generiska administratörskonton, inklusive bestämmelser om

   i) tilldelning av roller och ansvarsområden för att bevilja, granska och återkalla åtkomsträttigheter,

ii) tilldelning av privilegierad åtkomst, nödåtkomst och administratörsåtkomst efter behov eller från fall till fall och för samtliga IKT-system,

iii) återkallande av åtkomsträttigheter utan onödigt dröjsmål när anställningen upphör eller när åtkomsten inte längre är nödvändig,

iv) uppdatering av åtkomsträttigheter när ändringar krävs och minst en gång per år för samtliga IKT-system, utom för IKT-system som stöder kritiska eller viktiga funktioner där uppdateringen ska ske minst var sjätte månad.

(f) Autentiseringsmetoder, inklusive

i) användning av autentiseringsmetoder som står i proportion till den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554 och till IKT-tillgångarnas allmänna riskprofil och med beaktande av ledande praxis,

ii) användning av robusta metoder för autentisering i enlighet med ledande praxis och teknik för fjärråtkomst till den finansiella entitetens nätverk, för privilegierad åtkomst och för åtkomst till IKT-tillgångar som stöder kritiska eller viktiga funktioner eller IKT-tillgångar som är allmänt tillgängliga.

(g) Åtgärder för fysisk åtkomstkontroll, inklusive

i) identifiering och loggning av fysiska personer som är behöriga att få tillträde till lokaler, datacentraler och känsliga angivna områden som identifierats av den finansiella entiteten där IKT-tillgångar och informationstillgångar finns,

ii) beviljande av fysiska åtkomsträttigheter till kritiska IKT-tillgångar endast för behöriga personer, i enlighet med principerna om behovsenlig behörighet och minsta möjliga behörighet, och från fall till fall,

iii) övervakning av fysiskt tillträde till lokaler, datacentraler och känsliga angivna områden som identifierats av den finansiella entiteten där IKT-tillgångar och informationstillgångar eller bådadera finns,

iv) granskning av fysiska åtkomsträttigheter för att säkerställa att onödiga åtkomsträttigheter omedelbart återkallas.

Vid tillämpning av led e i ska finansiella entiteter fastställa lagringstiden med beaktande av verksamhets- och informationssäkerhetsmålen, skälen till att händelsen registreras i loggarna och resultaten av IKT-riskbedömningen.

Vid tillämpning av led e ii ska finansiella entiteter, när så är möjligt, använda särskilda konton för att utföra administrativa uppgifter på IKT-system. När så är möjligt och lämpligt ska finansiella entiteter införa automatiserade lösningar för hantering av privilegierad åtkomst.

Vid tillämpning av led g i ska identifieringen och loggningen stå i proportion till hur viktiga lokalerna, datacentralerna och de känsliga angivna områdena är och hur kritiska de verksamheter eller IKT-system som finns där är.

Vid tillämpning av led g iii ska övervakningen stå i proportion till den klassificering som fastställts i enlighet med artikel 8.1 i förordning (EU) 2022/2554 och hur kritiskt det område är till vilket åtkomst ges.

KAPITEL III
UPPTÄCKT OCH HANTERING AV IKT-RELATERADE INCIDENTER

Artikel 22
Policy för hantering av IKT-relaterade incidenter

Som en del av mekanismerna för att upptäcka onormal verksamhet, inbegripet frågor som rör IKT-nätverkens prestanda och IKT-relaterade incidenter, ska finansiella entiteter utarbeta, dokumentera och genomföra en policy för IKT-relaterade incidenter, genom vilken de ska

(a) dokumentera den process för hantering av IKT-relaterade incidenter som avses i artikel 17 i förordning (EU) 2022/2554,

(b) upprätta en förteckning över relevanta kontakter med interna funktioner och externa berörda parter som är direkt involverade i säkerheten för IKT-verksamhet, inbegripet för

  i) upptäckt och övervakning av cyberhot,

  ii) upptäckt av onormal verksamhet,

  iii) sårbarhetshantering,

(c) inrätta, genomföra och driva tekniska, organisatoriska och operativa mekanismer för att stödja processen för hantering av IKT-relaterade incidenter, inbegripet mekanismer för att möjliggöra en snabb upptäckt av onormal verksamhet och onormalt beteende i enlighet med artikel 23 i denna förordning,

(d) bevara all bevisning som rör IKT-relaterade incidenter under en period som inte ska vara längre än nödvändigt för de ändamål för vilka uppgifterna samlas in och står i proportion till hur kritiska de berörda affärsfunktionerna, stödprocesserna och IKT- och informationstillgångarna är, i enlighet med [artikel [15] i kommissionens delegerade förordning (EU) […]/[…] [kommissionens delegerade förordning om klassificering av IKT-relaterade incidenter][11] och med tillämpliga lagringskrav i enlighet med unionsrätten,

(e) inrätta och genomföra mekanismer för att analysera betydande eller återkommande IKT-relaterade incidenter och mönster i antalet och förekomsten av IKT-relaterade incidenter.

Vid tillämpning av led d ska finansiella entiteter bevara den bevisning som avses i det ledet på ett säkert sätt.

Artikel 23
Upptäckt av onormal verksamhet och kriterier för upptäckt och hantering av IKT-relaterade incidenter

1. Finansiella entiteter ska fastställa tydliga roller och ansvarsområden för att på ett ändamålsenligt sätt upptäcka och hantera IKT-relaterade incidenter och onormal verksamhet.

[11] (Publikationsbyrån: För in [hänvisning till och titel på denna delegerade förordning]).

2. Mekanismen för att snabbt upptäcka onormal verksamhet, inbegripet frågor som rör IKT-nätverkens prestanda och IKT-relaterade incidenter, som avses i artikel 10.1 i förordning (EU) 2022/2554, ska göra det möjligt för finansiella entiteter att

   (a) samla in, övervaka och analysera

      i) interna och externa faktorer, inklusive åtminstone de loggar som samlats in i enlighet med artikel 12 i denna förordning, information från affärsfunktioner och IKT-funktioner samt eventuella problem som rapporterats av användare av den finansiella entiteten,

      ii) potentiella interna och externa cyberhot, med beaktande av scenarier som vanligtvis används av fientliga aktörer och scenarier baserade på underrättelser om hot,

      iii) underrättelser från en tredjepartsleverantör av IKT-tjänster till den finansiella entiteten om IKT-relaterade incidenter som upptäckts i IKT-system och IKT-nätverk hos tredjepartsleverantören av IKT-tjänster och som kan beröra den finansiella entiteten,

   (b) identifiera onormal verksamhet och onormalt beteende, och införa verktyg som utfärdar varningar för onormal verksamhet och onormalt beteende, åtminstone för IKT-tillgångar och informationstillgångar som stöder kritiska eller viktiga funktioner,

   (c) prioritera de varningar som avses i led b för att möjliggöra hantering av de upptäckta IKT-relaterade incidenterna inom den förväntade åtgärdstiden, enligt vad som anges av finansiella entiteter, både under och utanför arbetstid,

   (d) registrera, analysera och utvärdera all relevant information om all onormal verksamhet och allt onormalt beteende automatiskt eller manuellt.

   Vid tillämpning av led b ska de verktyg som avses i det ledet innehålla verktyg som tillhandahåller automatiska varningar baserade på fördefinierade regler för att identifiera avvikelser som påverkar datakällornas eller logginsamlingens fullständighet och integritet.

3. Finansiella entiteter ska skydda all registrering av onormal verksamhet mot manipulering och obehörig åtkomst i vila, under överföring och, i relevanta fall, i bruk.

4. För varje upptäckt onormal verksamhet ska finansiella entiteter logga all relevant information, vilken möjliggör

   (a) identifiering av datum och tidpunkt för uppkomst av den onormala verksamheten,

   (b) identifiering av datum och tidpunkt för upptäckt av den onormala verksamheten,

   (c) identifiering av typen av onormal verksamhet.

5. Finansiella entiteter ska beakta samtliga följande kriterier för att utlösa de processer för upptäckt och hantering av IKT-relaterade incidenter som avses i artikel 10.2 i förordning (EU) 2022/2554:

   (a) Indikationer på att skadlig verksamhet kan ha utförts i ett IKT-system eller IKT-nätverk, eller att ett sådant IKT-system eller IKT-nätverk kan ha kompromitterats.

(b) Dataförluster som upptäcks när det gäller uppgifters tillgänglighet, äkthet, integritet och konfidentialitet.

(c) Upptäckt negativ påverkan på den finansiella entitetens transaktioner och verksamhet.

(d) IKT-systems och IKT-nätverks otillgänglighet.

6. Vid tillämpning av punkt 5 ska finansiella entiteter också beakta hur kritiska de berörda tjänsterna är.

KAPITEL IV
IKT-KONTINUITETSHANTERING

Artikel 24
Komponenter i IKT-kontinuitetspolicyn

1. Finansiella entiteter ska i sin IKT-kontinuitetspolicy som avses i artikel 11.1 i förordning (EU) 2022/2554 inkludera allt av följande:

(a) En beskrivning av

i) målen för IKT-kontinuitetspolicyn, inbegripet sambandet mellan IKT och övergripande kontinuitet, och med beaktande av resultaten av den verksamhetskonsekvensanalys som avses i artikel 11.5 i förordning (EU) 2022/2554,

ii) omfattningen av arrangemang, planer, förfaranden och mekanismer för IKT-kontinuitet, inklusive begränsningar och uteslutningar,

iii) den tidsram som ska täckas av arrangemangen, planerna, förfarandena och mekanismerna för IKT-kontinuitet,

iv) kriterierna för att aktivera och inaktivera IKT-kontinuitetsplaner, åtgärds- och återställningsplaner avseende IKT samt kriskommunikationsplaner.

(b) Bestämmelser om

i) styrning och organisation för att genomföra IKT-kontinuitetspolicyn, inklusive roller, ansvarsområden och eskaleringsförfaranden, som säkerställer att tillräckliga resurser finns tillgängliga,

ii) anpassning mellan IKT-kontinuitetsplanerna och de övergripande kontinuitetsplanerna, med avseende på åtminstone

1) scenarier för potentiella fel, inbegripet de scenarier som avses i artikel 26.2 i denna förordning,

2) återställningsmål, som anger att den finansiella entiteten ska kunna återställa driften av sina kritiska eller viktiga funktioner efter avbrott inom ett fastställt mål för återställningstid och ett fastställt mål för återställningspunkt,

iii) utarbetande av IKT-kontinuitetsplaner med allvarliga störningar i verksamheten som en del av dessa planer, och prioritering av IKT-kontinuitetsåtgärder med hjälp av en riskbaserad metod,

iv) utarbetande, testning och översyn av åtgärds- och återställningsplaner avseende IKT, i enlighet med artiklarna 25 och 26 i denna förordning,

v) granskning av ändamålsenligheten hos de genomförda arrangemangen, planerna, förfarandena och mekanismerna för IKT-kontinuitet, i enlighet med artikel 26 i denna förordning,

vi) anpassning av IKT-kontinuitetspolicyn till

1) den kommunikationsstrategi som avses i artikel 14.2 i förordning (EU) 2022/2554,

2) de kommunikations- och krishanteringsinsatser som avses i artikel 11.2 e i förordning (EU) 2022/2554.

2. Utöver de krav som avses i punkt 1 ska centrala motparter säkerställa att deras IKT-kontinuitetspolicy

(a) innehåller en maximal återställningstid för deras kritiska funktioner som inte är längre än två timmar,

(b) tar hänsyn till externa kopplingar och ömsesidiga beroenden inom de finansiella infrastrukturerna, inklusive handelsplatser som clearas av den centrala motparten, avvecklings- och betalningssystem för värdepapper samt kreditinstitut som används av den centrala motparten eller en anknuten central motpart,

(c) kräver att det finns arrangemang för att

i) säkerställa kontinuiteten för kritiska eller viktiga funktioner hos den centrala motparten baserat på katastrofscenarier,

ii) upprätthålla ett sekundärt driftställe som kan säkerställa kontinuiteten i kritiska eller viktiga funktioner hos den centrala motparten, vilket är identiskt med det primära driftstället,

iii) upprätthålla eller ha omedelbar tillgång till en reservplats för verksamheten, så att personalen kan säkerställa tjänstens kontinuitet om den primära verksamhetsplatsen inte är tillgänglig,

iv) överväga behovet av ytterligare driftställen, särskilt om de primära och sekundära driftställenas olika riskprofiler inte ger tillräckligt förtroende för att den centrala motpartens kontinuitetsmål kommer att uppfyllas i alla scenarier.

Vid tillämpning av led a ska centrala motparter under alla omständigheter slutföra förfaranden och betalningar vid dagens slut på utsatt tid och dag.

Vid tillämpning av led c i ska de arrangemang som avses i det ledet omfatta tillgång till tillräcklig personal, maximal längd för avbrott i kritiska funktioner, omkoppling och återställning till ett sekundärt driftställe.

Vid tillämpning av led c ii ska det sekundära driftställe som avses i det ledet ha en annan geografisk riskprofil än det primära driftstället.

3. Utöver de krav som avses i punkt 1 ska värdepapperscentraler säkerställa att deras IKT-kontinuitetspolicy

(a) tar hänsyn till eventuella kopplingar till och ömsesidiga beroenden med användare, kritiska försörjningstjänster och kritiska tjänsteleverantörer, andra värdepapperscentraler och andra marknadsinfrastrukturer,

(b) kräver att deras arrangemang för IKT-kontinuitet säkerställer att målet för återställningstiden för deras kritiska eller viktiga funktioner inte ska vara längre än två timmar.

4. Utöver de krav som avses i punkt 1 ska handelsplatser säkerställa att deras IKT-kontinuitetspolicy säkerställer att

(a) handeln kan återupptas inom eller strax efter två timmar efter en incident som orsakar störningar,

(b) den maximala mängden uppgifter som kan förloras från någon av handelsplatsens it-tjänster efter en incident som orsakar störningar är nära noll.

Artikel 25
Testning av IKT-kontinuitetsplanerna

1. När finansiella entiteter testar IKT-kontinuitetsplanerna i enlighet med artikel 11.6 i förordning (EU) 2022/2554 ska de ta hänsyn till den finansiella entitetens verksamhetskonsekvensanalys och den IKT-riskbedömning som avses i artikel 3 första stycket b i den här förordningen.

2. Finansiella entiteter ska genom testning av sina IKT-kontinuitetsplaner enligt punkt 1 bedöma om de kan säkerställa kontinuiteten i sina kritiska eller viktiga funktioner. Denna testning ska

(a) utföras på grundval av testscenarier som simulerar potentiella avbrott, inklusive en lämplig uppsättning allvarliga men troliga scenarier,

(b) innefatta IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster, i tillämpliga fall,

(c) för andra finansiella entiteter än mikroföretag enligt artikel 11.6 andra stycket i förordning (EU) 2022/2554, innehålla scenarier för byten från primär IKT-infrastruktur till reservkapacitet, säkerhetskopior och reservanläggningar,

(d) vara utformad för att pröva de antaganden som kontinuitetsplanerna bygger på, inbegripet styrningsarrangemang och kriskommunikationsplaner,

(e) innehålla förfaranden för att kontrollera förmågan hos de finansiella entiteternas personal, tredjepartsleverantörer av IKT-tjänster, IKT-system och IKT-tjänster att reagera på ett adekvat sätt på de scenarier som vederbörligen beaktas i enlighet med artikel 26.2.

Vid tillämpning av led a ska finansiella entiteter alltid inkludera de scenarier som beaktats vid utarbetandet av kontinuitetsplanerna i testerna.

Vid tillämpning av led b ska finansiella entiteter vederbörligen beakta scenarier kopplade till insolvens eller misslyckanden hos tredjepartsleverantörer av IKT-tjänster eller kopplade till politiska risker i tredjepartsleverantörernas jurisdiktioner, i relevanta fall.

Vid tillämpning av led c ska testningen verifiera om åtminstone kritiska eller viktiga funktioner kan drivas på lämpligt sätt under en tillräckligt lång tidsperiod och om den normala funktionen kan återställas.

3. Utöver de krav som avses i punkt 2 ska centrala motparter vid testningen av sina IKT-kontinuitetsplaner enligt punkt 1 involvera

(a) clearingmedlemmar,

(b) externa leverantörer,

(c) relevanta institut i den finansiella infrastrukturen med vilka de centrala motparterna har identifierat ömsesidiga beroenden i sina kontinuitetspolicyer.

4. Utöver de krav som avses i punkt 2 ska värdepapperscentraler vid testningen av sina IKT-kontinuitetsplaner enligt punkt 1 i tillämpliga fall involvera

(a) användare av värdepapperscentralerna,

(b) kritiska försörjningstjänster och kritiska tjänsteleverantörer,

(c) andra värdepapperscentraler,

(d) andra marknadsinfrastrukturer,

(e) alla andra institut med vilka värdepapperscentralerna har identifierat ömsesidiga beroenden i sin kontinuitetspolicy.

5. Finansiella entiteter ska dokumentera resultaten av den testning som avses i punkt 1. Alla brister som identifieras till följd av denna testning ska analyseras, åtgärdas och rapporteras till ledningsorganet.

Artikel 26
Åtgärds- och återställningsplaner avseende IKT

1. Vid utarbetandet av de åtgärds- och återställningsplaner avseende IKT som avses i artikel 11.3 i förordning (EU) 2022/2554 ska finansiella entiteter ta hänsyn till resultaten av den finansiella entitetens verksamhetskonsekvensanalys. Dessa åtgärds- och återställningsplaner avseende IKT ska

(a) ange de villkor som föranleder deras aktivering eller inaktivering, och eventuella undantag från sådan aktivering eller inaktivering,

(b) beskriva vilka åtgärder som ska vidtas för att säkerställa tillgänglighet, integritet och kontinuitet för och återställning av åtminstone IKT-system och IKT-tjänster som stöder kritiska eller viktiga funktioner hos den finansiella entiteten,

(c) vara utformade för att uppfylla återställningsmålen för de finansiella entiteternas verksamhet,

(d) dokumenteras och göras tillgängliga för den personal som är involverad i genomförandet av åtgärds- och återställningsplaner avseende IKT och vara lättillgängliga i nödsituationer,

(e) innehålla alternativ för återställning på både kort och lång sikt, inbegripet partiell systemåterställning,

(f) fastställa målen för åtgärds- och återställningsplaner avseende IKT och villkoren för att konstatera att dessa planer har genomförts på ett framgångsrikt sätt.

Vid tillämpning av led d ska finansiella entiteter tydligt ange roller och ansvarsområden.

2. De åtgärds- och återställningsplaner avseende IKT som avses i punkt 1 ska identifiera relevanta scenarier, inbegripet scenarier med allvarliga störningar i verksamheten och ökad sannolikhet för att störningar inträffar. Dessa planer ska utveckla scenarier baserade på aktuell information om hot och på lärdomar från

tidigare störningar i verksamheten. Finansiella entiteter ska vederbörligen beakta samtliga följande scenarier:

(a) Cyberangrepp och byten mellan primär IKT-infrastruktur och reservkapacitet, säkerhetskopior och reservanläggningar.

(b) Scenarier där kvaliteten på tillhandahållandet av en kritisk eller viktig funktion försämras till en oacceptabel nivå eller uteblir, och den potentiella effekten av insolvens, eller andra misslyckanden, hos någon relevant tredjepartsleverantör av IKT-tjänster.

(c) Partiellt eller totalt bortfall av lokaler, inklusive kontors- och affärslokaler samt datacentraler.

(d) Betydande fel på IKT-tillgångar eller på kommunikationsinfrastrukturen.

(e) Avsaknad av ett kritiskt antal anställda eller anställda som ansvarar för att garantera verksamhetens kontinuitet.

(f) Effekter av händelser relaterade till klimatförändringar och miljöförstöring, naturkatastrofer, pandemier och fysiska angrepp, inklusive intrång och terrorattentat.

(g) Angrepp inifrån.

(h) Politisk och social instabilitet, inklusive i relevanta fall inom tredjepartsleverantörens av IKT-tjänster jurisdiktion och på den plats där uppgifter lagras och behandlas.

(i) Omfattande strömavbrott.

3. Om de primära återställningsåtgärderna kanske inte är genomförbara på kort sikt på grund av kostnader, risker, logistik eller oförutsedda omständigheter, ska de åtgärds- och återställningsplaner avseende IKT som avses i punkt 1 överväga alternativa möjligheter.

4. Som en del av de åtgärds- och återställningsplaner avseende IKT som avses i punkt 1 ska finansiella entiteter överväga och genomföra kontinuitetsåtgärder för att begränsa misslyckanden hos tredjepartsleverantörer av IKT-tjänster att tillhandahålla IKT-tjänster som stöder kritiska eller viktiga funktioner hos den finansiella entiteten.

KAPITEL V
RAPPORT OM ÖVERSYNEN AV IKT-RISKHANTERINGSRAMEN

Artikel 27

Formatet för och innehållet i rapporten om översynen av IKT-riskhanteringsramen

1. Finansiella entiteter ska lämna in den rapport om översynen av IKT-riskhanteringsramen som avses i artikel 6.5 i förordning (EU) 2022/2554 i ett sökbart elektroniskt format.

2. Finansiella entiteter ska ta med all följande information i den rapport som avses i punkt 1:

(a) Ett inledande avsnitt som

i) tydligt identifierar den finansiella entitet som är föremål för rapporten och beskriver dess koncernstruktur, där så är relevant,

ii) beskriver bakgrunden till rapporten med avseende på karaktären på, omfattningen av och komplexiteten i den finansiella entitetens tjänster, verksamhet och insatser, den finansiella entitetens organisation, identifierade kritiska funktioner, strategi, större pågående projekt eller aktiviteter, relationer och beroende av interna och utkontrakterade IKT-tjänster och IKT-system eller de konsekvenser som en total förlust eller allvarlig försämring av sådana system skulle få med avseende på kritiska eller viktiga funktioner och marknadseffektivitet,

iii) sammanfattar de större förändringarna i IKT-riskhanteringsramen sedan den föregående inlämnade rapporten,

iv) på verkställande nivå sammanfattar den aktuella IKT-riskprofilen och IKT-riskprofilen för närmare tid, hotbilden, den bedömda effektiviteten av dess kontroller och den finansiella entitetens säkerhetsstatus.

(b) Datum för godkännande av rapporten av den finansiella entitetens ledningsorgan.

(c) En beskrivning av skälet till översynen av IKT-riskhanteringsramen i enlighet med artikel 6.5 i förordning (EU) 2022/2554.

(d) Start- och slutdatum för översynsperioden.

(e) En uppgift om vilken funktion som ansvarar för översynen.

(f) En beskrivning av större förändringar och förbättringar av IKT-riskhanteringsramen sedan den föregående översynen.

(g) En sammanfattning av resultaten av översynen och en detaljerad analys och bedömning av hur allvarliga svagheterna, bristerna och luckorna i IKT-riskhanteringsramen har varit under översynsperioden.

(h) En beskrivning av åtgärderna för att hantera identifierade svagheter, brister och luckor, inklusive

i) en sammanfattning av de åtgärder som vidtagits för att avhjälpa identifierade svagheter, brister och luckor,

ii) ett förväntat datum för genomförande av åtgärderna och datum för den interna kontrollen av genomförandet, inklusive information om hur långt genomförandet av dessa åtgärder har kommit vid tidpunkten för upprättandet av rapporten och i tillämpliga fall med uppgift om huruvida det finns en risk för att tidsfristerna inte kan hållas,

iii) verktyg som ska användas och identifiering av den funktion som ansvarar för att genomföra åtgärderna, med angivande av om verktygen och funktionerna är interna eller externa,

iv) en beskrivning av hur de förändringar som planeras i åtgärderna påverkar den finansiella entitetens budgetmedel, personalresurser och materiella resurser, inklusive resurser som avsatts för genomförandet av eventuella korrigerande åtgärder,

v) information om processen för att informera den behöriga myndigheten, i relevanta fall,

vi) om de identifierade svagheterna, bristerna eller luckorna inte är föremål för korrigerande åtgärder, en detaljerad beskrivning av de kriterier som används för att analysera effekterna av dessa svagheter, brister eller luckor, för att utvärdera den relaterade kvarstående IKT-risken och för att acceptera den relaterade kvarstående risken.

(i) Information om planerad vidareutveckling av IKT-riskhanteringsramen.

(j) Slutsatser från översynen av IKT-riskhanteringsramen.

(k) Information om tidigare översyner, inklusive

i) en förteckning över tidigare gjorda översyner,

ii) i tillämpliga fall, en lägesrapport om genomförandet av de korrigerande åtgärder som identifierades i den senaste rapporten,

iii) om de föreslagna korrigerande åtgärderna i tidigare översyner har visat sig vara ineffektiva eller har inneburit oväntade utmaningar, en beskrivning av hur dessa korrigerande åtgärder skulle kunna förbättras eller av dessa oväntade utmaningar.

(l) Informationskällor som använts vid utarbetandet av rapporten, inklusive

i) för andra finansiella entiteter än mikroföretag enligt artikel 6.6 i förordning (EU) 2022/2554, resultaten av internrevisioner,

ii) resultaten av bedömningar av efterlevnaden,

iii) resultaten av testning av digital operativ motståndskraft, och i tillämpliga fall resultaten av avancerad testning, baserad på hotbildsstyrd penetrationstestning, av IKT-verktyg, IKT-system och IKT-processer,

iv) externa källor.

Vid tillämpning av led c ska rapporten, om översynen initierades till följd av tillsynsinstruktioner eller slutsatser från relevanta testningsprocesser för digital operativ motståndskraft eller revisionsprocesser, innehålla uttryckliga hänvisningar till sådana instruktioner eller slutsatser, vilket gör det möjligt att identifiera skälet till att översynen initierades. Om översynen initierades med anledning av IKT-relaterade incidenter ska rapporten innehålla en förteckning över alla IKT-relaterade incidenter med en analys av grundorsaken till respektive incident.

Vid tillämpning av led f ska beskrivningen innehålla en analys av förändringarnas inverkan på den finansiella entitetens strategi för digital operativ motståndskraft, på den finansiella entitetens interna IKT-kontrollram och på den finansiella entitetens styrning av IKT-riskhantering.

AVDELNING III – FÖRENKLAD IKT-RISKHANTERINGSRAM FÖR FINANSIELLA ENTITETER SOM AVSES I ARTIKEL 16.1 I FÖRORDNING (EU) 2022/2554

KAPITEL I
FÖRENKLAD IKT-RISKHANTERINGSRAM

Artikel 28
Styrning och organisation

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska ha en intern styrnings- och kontrollram som säkerställer en ändamålsenlig och ansvarsfull hantering av IKT-risker i syfte att åstadkomma en hög nivå av digital operativ motståndskraft.

2. De finansiella entiteter som avses i punkt 1 ska, som en del av sin förenklade IKT-riskhanteringsram, säkerställa att deras ledningsorgan

   (a) bär det övergripande ansvaret för att säkerställa att den förenklade IKT-riskhanteringsramen gör det möjligt att uppnå den finansiella entitetens affärsstrategi i enlighet med den finansiella entitetens riskbenägenhet, och säkerställer att IKT-risken beaktas i detta sammanhang,

   (b) fastställer tydliga roller och ansvarsområden för alla IKT-relaterade uppgifter,

   (c) fastställer informationssäkerhetsmål och IKT-krav,

   (d) godkänner, övervakar och regelbundet ser över

      i) klassificeringen av den finansiella enhetens informationstillgångar som avses i artikel 30.1 i denna förordning, förteckningen över identifierade huvudrisker samt verksamhetskonsekvensanalysen och tillhörande policyer,

      ii) den finansiella entitetens kontinuitetsplaner och de åtgärds- och återställningsåtgärder som avses i artikel 16.1 f i förordning (EU) 2022/2554,

   (e) minst en gång per år anslår och ser över den budget som krävs för att uppfylla den finansiella entitetens behov av digital operativ motståndskraft när det gäller alla typer av resurser, inbegripet relevanta program för medvetenhet om IKT-säkerhet och utbildning i digital operativ motståndskraft samt IKT-färdigheter för all personal,

   (f) specificerar och genomför de policyer och åtgärder som anges i kapitlen I, II och III i denna avdelning för att identifiera, bedöma och hantera den IKT-risk som den finansiella entiteten är exponerad för,

   (g) identifierar och genomför förfaranden, IKT-protokoll och verktyg som är nödvändiga för att skydda alla informationstillgångar och IKT-tillgångar,

   (h) säkerställer att den finansiella entitetens personal hålls uppdaterad med tillräckliga kunskaper och färdigheter för att förstå och bedöma IKT-risker och

deras inverkan på den finansiella entitetens verksamhet, i proportion till den IKT-risk som hanteras,

(i) upprättar rapporteringsarrangemang, inbegripet hur ofta, i vilken form och med vilket innehåll rapportering till ledningsorganet om informationssäkerheten och den digitala operativa motståndskraften ska ske.

3. De finansiella entiteter som avses i punkt 1 får, i enlighet med unionsrätten och den nationella rätten på området, utkontraktera uppgiften att kontrollera efterlevnaden av IKT-riskhanteringskraven på koncerninterna IKT-leverantörer eller tredjepartsleverantörer av IKT-tjänster. Vid sådan utkontraktering ska de finansiella entiteterna förbli fullt ansvariga för kontrollen av efterlevnaden av IKT-riskhanteringskraven.

4. De finansiella entiteter som avses i punkt 1 ska säkerställa lämplig åtskillnad av och oberoende för kontrollfunktioner och interna revisionsfunktioner.

5. De finansiella entiteter som avses i punkt 1 ska säkerställa att deras förenklade IKT-riskhanteringsram är föremål för en internrevision av revisorer, i linje med de finansiella entiteternas revisionsplan. Revisorerna ska ha tillräckliga kunskaper och färdigheter och tillräcklig expertis om IKT-risker och ska vara oberoende. IKT-revisionernas frekvens och inriktning ska stå i proportion till den finansiella entitetens IKT-risk.

6. På grundval av resultatet av den revision som avses i punkt 5 ska de finansiella entiteter som avses i punkt 1 säkerställa att kritiska IKT-revisionsresultat verifieras och åtgärdas skyndsamt.

Artikel 29
Riktlinjer och åtgärder för informationssäkerhet

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska utarbeta, dokumentera och genomföra riktlinjer för informationssäkerhet i samband med den förenklade IKT-riskhanteringsramen. I riktlinjerna för informationssäkerhet ska det anges vilka principer och regler på hög nivå som ska skydda konfidentialitet, integritet, tillgänglighet och äkthet för uppgifter och för de tjänster som dessa finansiella entiteter tillhandahåller.

2. På grundval av sina riktlinjer för informationssäkerhet enligt punkt 1 ska de finansiella entiteter som avses i punkt 1 fastställa och genomföra IKT-säkerhetsåtgärder för att minska sin exponering för IKT-risker, inbegripet begränsningsåtgärder som genomförs av tredjepartsleverantörer av IKT-tjänster.

IKT-säkerhetsåtgärderna ska omfatta alla de åtgärder som avses i artiklarna 30–38.

Artikel 30
Klassificering av informationstillgångar och IKT-tillgångar

1. Som en del av den förenklade IKT-riskhanteringsram som avses i artikel 16.1 a i förordning (EU) 2022/2554 ska de finansiella entiteter som avses i punkt 1 i den artikeln identifiera, klassificera och dokumentera alla kritiska eller viktiga funktioner, de informationstillgångar och IKT-tillgångar som stöder dem och deras ömsesidiga beroenden. Finansiella entiteter ska vid behov se över denna identifiering och klassificering.

2. De finansiella entiteter som avses i punkt 1 ska identifiera alla kritiska eller viktiga funktioner som stöds av tredjepartsleverantörer av IKT-tjänster.

Artikel 31
IKT-riskhantering

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska i sin förenklade IKT-riskhanteringsram inkludera allt av följande:

   (a) Ett fastställande av risktoleransnivåerna för IKT-risker, i enlighet med den finansiella entitetens riskbenägenhet.

   (b) Identifiering och bedömning av de IKT-risker som den finansiella entiteten är exponerad för.

   (c) Specificering av begränsningsstrategier för åtminstone de IKT-risker som inte ligger inom den finansiella entitetens risktoleransnivåer.

   (d) Övervakning av effektiviteten hos de begränsningsstrategier som avses i led c.

   (e) Identifiering och bedömning av eventuella IKT-risker och informationssäkerhetsrisker till följd av större förändringar i IKT-system eller IKT-tjänster, processer eller förfaranden, och från resultat av IKT-säkerhetstester och efter en allvarlig IKT-relaterad incident.

2. De finansiella entiteter som avses i punkt 1 ska regelbundet genomföra och dokumentera IKT-riskbedömningen i proportion till de finansiella entiteternas IKT-riskprofil.

3. De finansiella entiteter som avses i punkt 1 ska kontinuerligt övervaka hot och sårbarheter som är relevanta för deras kritiska eller viktiga funktioner, och informationstillgångar och IKT-tillgångar, och ska regelbundet se över de riskscenarier som berör dessa kritiska eller viktiga funktioner.

4. De finansiella entiteter som avses i punkt 1 ska fastställa varningströskelvärden och kriterier för att utlösa och initiera processer för hantering av IKT-relaterade incidenter.

Artikel 32
Fysisk säkerhet och miljösäkerhet

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska identifiera och genomföra fysiska säkerhetsåtgärder som utformats på grundval av hotbilden och i enlighet med den klassificering som avses i artikel 30.1 i den här förordningen, den allmänna riskprofilen för IKT-tillgångar och tillgängliga informationstillgångar.

2. De åtgärder som avses i punkt 1 ska skydda finansiella entiteters lokaler och, i tillämpliga fall, finansiella entiteters datacentraler där IKT-tillgångar och informationstillgångar finns, mot obehörig åtkomst, angrepp och olyckor samt mot miljöhot och miljöfaror.

3. Skyddet mot miljöhot och miljöfaror ska stå i proportion till hur viktiga de berörda lokalerna och, i tillämpliga fall, datacentralerna är och hur kritiska de verksamheter eller IKT-system som finns där är.

KAPITEL II
YTTERLIGARE DELAR AV SYSTEM, PROTOKOLL OCH VERKTYG FÖR ATT MINIMERA EFFEKTERNA AV IKT-RISK

Artikel 33
Åtkomstkontroll

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska utarbeta, dokumentera och genomföra förfaranden för kontroll av logisk och fysisk åtkomst och ska kontrollera efterlevnaden av, övervaka och regelbundet se över dessa förfaranden. Dessa förfaranden ska innehålla följande delar av kontrollen av logisk och fysisk åtkomst:

   (a) Åtkomsträttigheter till informationstillgångar, IKT-tillgångar och de funktioner som stöds av dem, samt till kritiska platser för den finansiella entitetens verksamhet, som ska hanteras enligt principerna om behovsenlig behörighet, behovsenlig användning och minsta möjliga behörighet, inklusive för fjärråtkomst och nödåtkomst.

   (b) Användaransvar, vilket säkerställer att användare kan identifieras när åtgärder utförs i IKT-systemen.

   (c) Förfaranden för kontohantering för att bevilja, ändra eller återkalla åtkomsträttigheter för användarkonton och generiska konton, även generiska administratörskonton.

   (d) Autentiseringsmetoder som står i proportion till den klassificering som avses i artikel 30.1 och till IKT-tillgångarnas allmänna riskprofil, och som bygger på ledande praxis.

   (e) Regelbunden översyn av åtkomsträttigheter och återkallande av dem när de inte längre behövs.

   Vid tillämpning av led c ska den finansiella entiteten tilldela privilegierad åtkomst, nödåtkomst och administratörsåtkomst efter behov eller från fall till fall och för samtliga IKT-system, och åtkomsten ska loggas i enlighet med artikel 34 första stycket f.

   Vid tillämpning av led d ska finansiella entiteter använda robusta metoder för autentisering som bygger på ledande praxis för fjärråtkomst till den finansiella entitetens nätverk, för privilegierad åtkomst och för åtkomst till IKT-tillgångar som stöder kritiska eller viktiga funktioner och som är allmänt tillgängliga.

Artikel 34
Säkerhet för IKT-verksamhet

De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska, som en del av sina system, protokoll och verktyg, och för alla IKT-tillgångar

(a) övervaka och hantera livscykeln för alla IKT-tillgångar,

(b) övervaka huruvida IKT-tillgångarna stöds av finansiella entiteters tredjepartsleverantörer av IKT-tjänster, i tillämpliga fall,

(c) identifiera kapacitetskrav för sina IKT-tillgångar och åtgärder för att upprätthålla och förbättra tillgängligheten och effektiviteten hos IKT-system och förhindra brist på IKT-kapacitet innan den uppstår,

(d) utföra automatiserade sårbarhetsbedömningar och bedömningar av IKT-tillgångar i proportion till deras klassificering enligt artikel 30.1 och till IKT-tillgångens allmänna riskprofil, samt införa programfixar för att åtgärda identifierade sårbarheter,

(e) hantera riskerna med föråldrade, ej stödda eller äldre IKT-tillgångar,

(f) logga händelser relaterade till logisk och fysisk åtkomstkontroll, IKT-verksamhet, inklusive system- och nätverkstrafik, och hantering av IKT-förändringar,

(g) identifiera och genomföra åtgärder för att övervaka och analysera information om onormal verksamhet och onormalt beteende för kritisk eller viktig IKT-verksamhet,

(h) genomföra åtgärder för att övervaka relevant och uppdaterad information om cyberhot,

(i) genomföra åtgärder för att identifiera möjliga informationsläckor, skadlig kod och andra säkerhetshot samt allmänt kända sårbarheter i programvara och hårdvara, och kontrollera om det finns motsvarande nya säkerhetsuppdateringar.

Vid tillämpning av led f ska finansiella entiteter anpassa loggarnas detaljnivå till sitt syfte och användningen av den IKT-tillgång som producerar dessa loggar.

Artikel 35
Data-, system- och nätverkssäkerhet

De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska, som en del av sina system, protokoll och verktyg, utveckla och genomföra skyddsåtgärder som säkerställer nätverkens säkerhet mot intrång och missbruk av uppgifter och som bevarar uppgifters tillgänglighet, äkthet, integritet och konfidentialitet. I synnerhet ska finansiella entiteter, med beaktande av den klassificering som avses i artikel 30.1 i denna förordning, fastställa allt av följande:

(a) Identifiering och genomförande av åtgärder för att skydda uppgifter i bruk, under överföring och i vila.

(b) Identifiering och genomförande av säkerhetsåtgärder avseende användning av programvara, datalagringsmedier, system och slutpunktsenheter som överför och lagrar den finansiella entitetens uppgifter.

(c) Identifiering och genomförande av åtgärder för att förhindra och upptäcka obehöriga anslutningar till den finansiella entitetens nätverk, och för att säkra nätverkstrafiken mellan den finansiella entitetens interna nätverk och internet och andra externa anslutningar.

(d) Identifiering och genomförande av åtgärder som säkerställer tillgänglighet, äkthet, integritet och konfidentialitet för uppgifter under överföring i nätverk.

(e) En process för att på ett säkert sätt radera uppgifter som finns i lokalerna, eller som lagras externt, och som den finansiella entiteten inte längre behöver samla in eller lagra.

(f) En process för att på ett säkert sätt bortskaffa eller obrukbargöra datalagringsenheter som finns i lokalerna, eller datalagringsenheter som lagras externt, vilka innehåller konfidentiell information.

(g) Identifiering och genomförande av åtgärder för att säkerställa att distansarbete och användning av privata slutpunktsenheter inte negativt påverkar den finansiella entitetens förmåga att utföra sin kritiska verksamhet på ett adekvat, snabbt och säkert sätt.

Artikel 36
IKT-säkerhetstestning

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska upprätta och genomföra en plan för IKT-säkerhetstestning i syfte att validera ändamålsenligheten hos sina IKT-säkerhetsåtgärder som utvecklats i enlighet med artiklarna 33, 34 och 35 samt artiklarna 37 och 38 i den här förordningen. Finansiella entiteter ska säkerställa att den planen beaktar hot och sårbarheter som identifierats som en del av den förenklade IKT-riskhanteringsram som avses i artikel 31 i denna förordning.

2. De finansiella entiteter som avses i punkt 1 ska se över, bedöma och testa IKT-säkerhetsåtgärder, med beaktande av den allmänna riskprofilen för den finansiella entitetens IKT-tillgångar.

3. De finansiella entiteter som avses i punkt 1 ska övervaka och utvärdera resultaten av säkerhetstesterna och uppdatera sina säkerhetsåtgärder i enlighet därmed, och utan onödigt dröjsmål när det gäller IKT-system som stöder kritiska eller viktiga funktioner.

Artikel 37
Förvärv, utveckling och underhåll av IKT-system

De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska, när så är lämpligt, utforma och genomföra ett förfarande som styr förvärv, utveckling och underhåll av IKT-system enligt en riskbaserad metod. Detta förfarande ska

(a) säkerställa att de funktionella och icke-funktionella kraven, inbegripet kraven på informationssäkerhet, är tydligt specificerade och godkända av den berörda affärsfunktionen, innan något förvärv eller någon utveckling av IKT-system äger rum,

(b) säkerställa testning och godkännande av IKT-system innan de används för första gången och innan ändringar av IKT-systemet införs i produktionsmiljön,

(c) identifiera åtgärder för att minska risken för oavsiktlig ändring eller avsiktlig manipulering av IKT-systemen under utveckling och införande i produktionsmiljön.

Artikel 38
IKT-projekthantering och hantering av IKT-förändringar

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska utveckla, dokumentera och genomföra ett förfarande för IKT-projekthantering och ska specificera roller och ansvarsområden för dess genomförande. Detta förfarande ska omfatta alla stadier av IKT-projekten från deras initiering till deras avslutande.

2. De finansiella entiteter som avses i punkt 1 ska utveckla, dokumentera och genomföra ett förfarande för hantering av IKT-förändringar för att säkerställa att alla ändringar av IKT-system registreras, testas, bedöms, godkänns, genomförs och verifieras på ett kontrollerat sätt och med lämpliga skyddsåtgärder för att bevara den finansiella entitetens digitala operativa motståndskraft.

Kapitel III
IKT-KONTINUITETSHANTERING

Artikel 39
Komponenter i IKT-kontinuitetsplanen

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska utarbeta sina IKT-kontinuitetsplaner med beaktande av resultaten av analysen av deras exponering för och potentiella effekter av allvarliga störningar i verksamheten och scenarier som deras IKT-tillgångar som stöder kritiska eller viktiga funktioner kan utsättas för, inbegripet ett scenario för cyberangrepp.

2. De IKT-kontinuitetsplaner som avses i punkt 1 ska

   (a) godkännas av den finansiella entitetens ledningsorgan,

   (b) vara dokumenterade och lättillgängliga i händelse av en nödsituation eller kris,

   (c) avsätta tillräckliga resurser för deras genomförande,

   (d) fastställa planerade återställningsnivåer och tidsramar för återställning och återupptagande av funktioner och viktiga interna och externa beroenden, inklusive tredjepartsleverantörer av IKT-tjänster,

   (e) identifiera de förhållanden som kan föranleda aktivering av IKT-kontinuitetsplanerna och vilka åtgärder som ska vidtas för att säkerställa tillgänglighet och kontinuitet för och återställning av de finansiella entiteternas IKT-tillgångar som stöder kritiska eller viktiga funktioner,

   (f) identifiera åtgärder för återskapande och återställning av kritiska eller viktiga affärsfunktioner, stödprocesser och informationstillgångar och deras ömsesidiga beroenden, för att undvika negativa effekter på de finansiella entiteternas funktion,

   (g) identifiera förfaranden och åtgärder för säkerhetskopiering som anger omfattningen av de uppgifter som ska säkerhetskopieras och den lägsta frekvensen för säkerhetskopieringen, baserat på hur kritisk den funktion som använder dessa uppgifter är,

   (h) överväga alternativ där återställning kanske inte är genomförbar på kort sikt på grund av kostnader, risker, logistik eller oförutsedda omständigheter,

   (i) specificera interna och externa kommunikationsarrangemang, inklusive eskaleringsplaner,

   (j) uppdateras i linje med lärdomar från incidenter, tester, nya risker och hot som identifierats, ändrade återställningsmål, större förändringar av den finansiella entitetens organisation och av de IKT-tillgångar som stöder kritiska funktioner eller affärsfunktioner.

Vid tillämpning av led f ska de åtgärder som avses i det ledet föreskriva begränsning av misslyckanden hos kritiska tredjepartsleverantörer.

Artikel 40
Testning av kontinuitetsplaner

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska testa sina kontinuitetsplaner som avses i artikel 39 i den här förordningen, inbegripet de scenarier som avses i den artikeln, minst en gång om året i fråga om förfarandena för säkerhetskopiering och återskapande, eller vid varje större förändring av kontinuitetsplanen.

2. Den testning av kontinuitetsplaner som avses i punkt 1 ska visa att de finansiella entiteter som avses i den punkten kan upprätthålla bärkraftigheten i sin verksamhet till dess att kritisk verksamhet har återupprättats och identifiera eventuella brister i dessa planer.

3. De finansiella entiteter som avses i punkt 1 ska dokumentera resultaten av testningen av kontinuitetsplanerna, och alla brister som identifieras till följd av denna testning ska analyseras, åtgärdas och rapporteras till ledningsorganet.

KAPITEL IV
RAPPORT OM ÖVERSYNEN AV DEN FÖRENKLADE IKT-RISKHANTERINGSRAMEN

Artikel 41
Formatet för och innehållet i rapporten om översynen av den förenklade IKT-riskhanteringsramen

1. De finansiella entiteter som avses i artikel 16.1 i förordning (EU) 2022/2554 ska lämna den rapport om översynen av IKT-riskhanteringsramen som avses i punkt 2 i den artikeln i ett sökbart elektroniskt format.

2. Den rapport som avses i punkt 1 ska innehålla all följande information:

   (a) Ett inledande avsnitt som innehåller

      i) en beskrivning av bakgrunden till rapporten med avseende på karaktären på, omfattningen av och komplexiteten i den finansiella entitetens tjänster, verksamhet och insatser, den finansiella entitetens organisation, identifierade kritiska funktioner, strategi, större pågående projekt eller aktiviteter och relationer, och den finansiella entitetens beroende av interna och utkontrakterade IKT-tjänster och IKT-system eller de konsekvenser som en total förlust eller allvarlig försämring av sådana system skulle få för kritiska eller viktiga funktioner och marknadseffektivitet,

      ii) en sammanfattning på verkställande nivå av den aktuella IKT-risk och IKT-risk för närmare tid som identifierats, hotbilden, den bedömda effektiviteten av dess kontroller och den finansiella entitetens säkerhetsstatus,

      iii) information om det rapporterade området,

iv) en sammanfattning av de större förändringarna i IKT-riskhanteringsramen sedan den föregående rapporten,

v) en sammanfattning och beskrivning av effekterna av de större förändringarna i den förenklade IKT-riskhanteringsramen sedan den föregående rapporten.

(b) I tillämpliga fall, datum för godkännande av rapporten av den finansiella entitetens ledningsorgan.

(c) En beskrivning av skälen till översynen, inklusive

i) om översynen har initierats efter tillsynsinstruktioner, bevisning för sådana instruktioner,

ii) om översynen har initierats efter IKT-relaterade incidenter, en förteckning över alla dessa IKT-relaterade incidenter med tillhörande analys av grundorsaken till respektive incident.

(d) Start- och slutdatum för översynsperioden.

(e) Den person som ansvarar för översynen.

(f) En sammanfattning av resultaten och en självutvärdering av allvarlighetsgraden hos de svagheter, brister och luckor som identifierats i IKT-riskhanteringsramen för översynsperioden, inklusive en detaljerad analys av dessa.

(g) Identifierade åtgärder för att avhjälpa svagheter, brister och luckor i den förenklade IKT-riskhanteringsramen, och förväntat datum för genomförande av dessa åtgärder, inbegripet uppföljning av svagheter, brister och luckor som identifierats i föregående rapporter, om dessa svagheter, brister och luckor ännu inte har avhjälpts.

(h) Övergripande slutsatser om översynen av den förenklade IKT-riskhanteringsramen, inklusive ytterligare planerad utveckling.

AVDELNING IV – SLUTBESTÄMMELSER

Artikel 42
Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 13.3.2024

På kommissionens vägnar
Ordförande
Ursula VON DER LEYEN